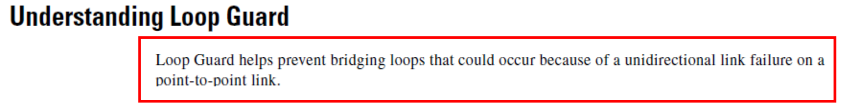
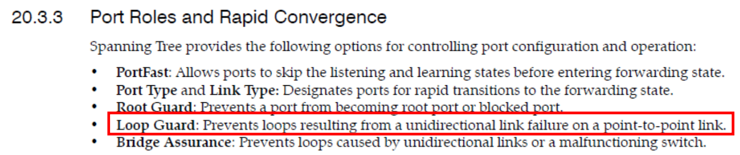
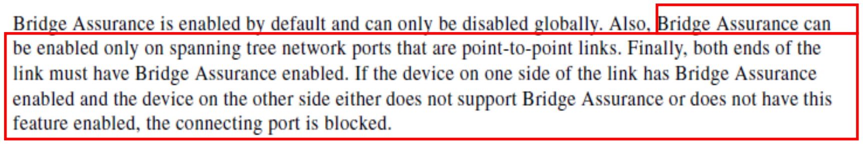
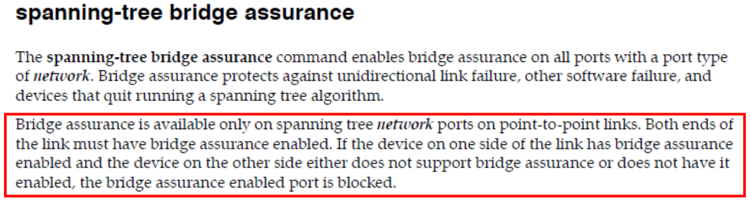
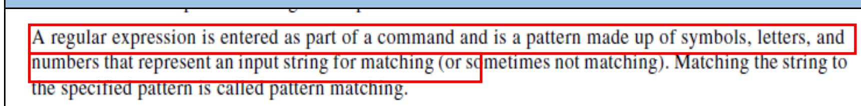
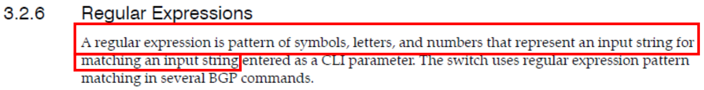
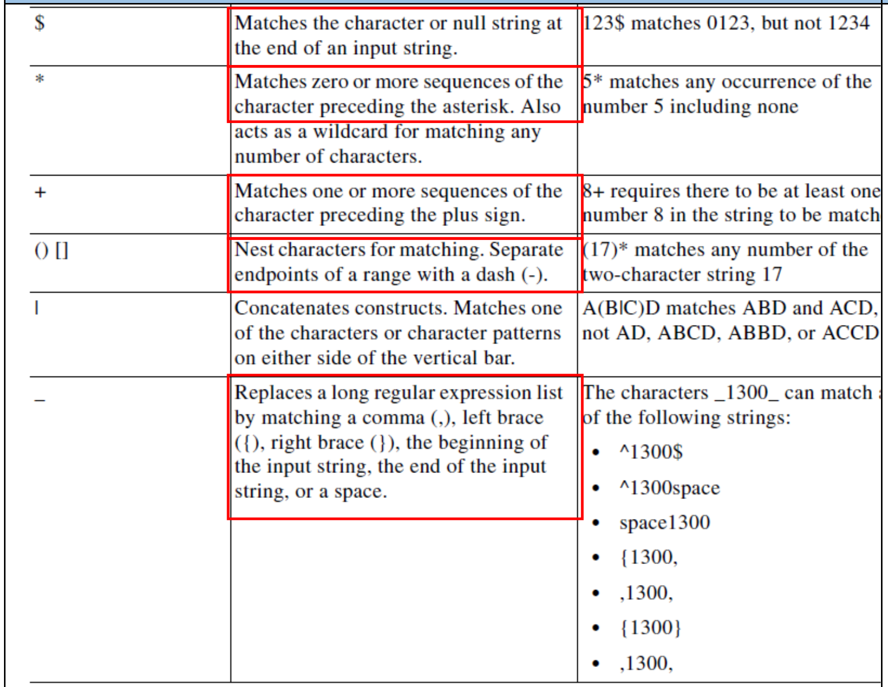
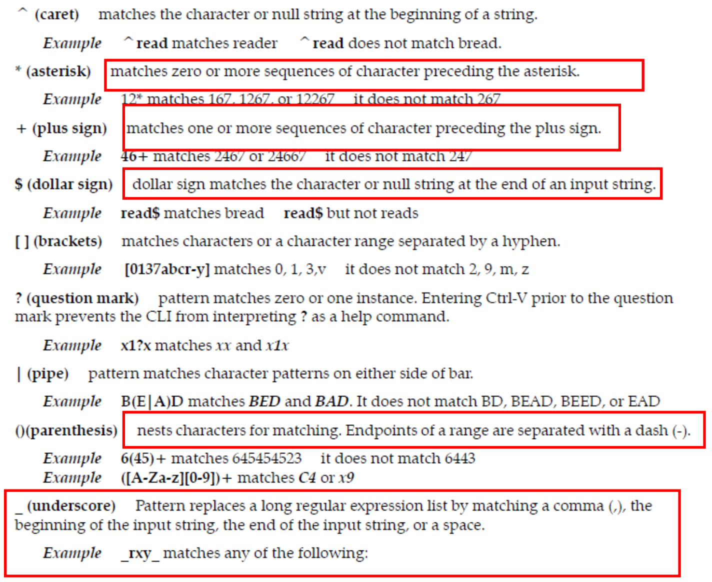
EXHIBITS A1-A6

(Part 4 of 13)

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Understanding Loop Guard** Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link. Cisco NX-OS Layer 2 Switching Configuration Guide (2008), Release 4.0, at 7-6.	 20.3.3 Port Roles and Rapid Convergence Spanning Tree provides the following options for controlling port configuration and operation: • **PortFast**: Allows ports to skip the listening and learning states before entering forwarding state. • **Port Type** and **Link Type:** Designates ports for rapid transitions to the forwarding state. • **Root Guard**: Prevents a port from becoming root port or blocked port. • **Loop Guard**: Prevents loops resulting from a unidirectional link failure on a point-to-point link. • **Bridge Assurance**: Prevents loops caused by unidirectional links or a malfunctioning switch. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 964. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 842; Arista User Manual, v. 4.11.1 (1/11/13), at 660; Arista User Manual v. 4.10.3 (10/22/12), at 574; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.	Dkt. 419-10 at PDF p. 104
 Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked. Cisco NX-OS Layer 2 Switching Configuration Guide (2008), Release 4.0, at 7-3.	 **spanning-tree bridge assurance** The **spanning-tree bridge assurance** command enables bridge assurance on all ports with a port type of ***network***. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm. Bridge assurance is available only on spanning tree ***network*** ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1002. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.	Dkt. 419-10 at PDF p. 104

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 A regular expression is entered as part of a command and is a pattern made up of symbols, letters, and numbers that represent an input string for matching (or sometimes not matching). Matching the string to the specified pattern is called pattern matching. Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at A-1.	 3.2.6 Regular Expressions A regular expression is pattern of symbols, letters, and numbers that represent an input string for matching an input string entered as a CLI parameter. The switch uses regular expression pattern matching in several BGP commands. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 106. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 94; Arista User Manual, v. 4.11.1 (1/11/13), at 64; Arista User Manual v. 4.10.3 (10/22/12), at 56; Arista User Manual v. 4.9.3.2 (5/3/12), at 52; Arista User Manual v. 4.8.2 (11/18/11), at 48.	Dkt. 419-10 at PDF p. 105

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

<table>
<tr><td>$</td><td>Matches the character or null string at the end of an input string.</td><td>123$ matches 0123, but not 1234</td></tr>
<tr><td>*</td><td>Matches zero or more sequences of the character preceding the asterisk. Also acts as a wildcard for matching any number of characters.</td><td>5* matches any occurrence of the number 5 including none</td></tr>
<tr><td>+</td><td>Matches one or more sequences of the character preceding the plus sign.</td><td>8+ requires there to be at least one number 8 in the string to be match</td></tr>
<tr><td>() []</td><td>Nest characters for matching. Separate endpoints of a range with a dash (-).</td><td>(17)* matches any number of the two-character string 17</td></tr>
<tr><td>|</td><td>Concatenates constructs. Matches one of the characters or character patterns on either side of the vertical bar.</td><td>A(B|C)D matches ABD and ACD, not AD, ABCD, ABBD, or ACCD</td></tr>
<tr><td>_</td><td>Replaces a long regular expression list by matching a comma (,), left brace ({), right brace (}), the beginning of the input string, the end of the input string, or a space.</td><td>The characters _1300_ can match of the following strings:
• ^1300$
• ^1300space
• space1300
• {1300,
• ,1300,
• {1300}
• ,1300,</td></tr>
</table>

Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at A-2.
</td>
<td>


^ (caret) matches the character or null string at the beginning of a string.

Example ^read matches reader ^read does not match bread.

* (asterisk) matches zero or more sequences of character preceding the asterisk.

Example 12* matches 167, 1267, or 12267 it does not match 267

+ (plus sign) matches one or more sequences of character preceding the plus sign.

Example 46+ matches 2467 or 24667 it does not match 247

$ (dollar sign) dollar sign matches the character or null string at the end of an input string.

Example read$ matches bread read$ but not reads

[ ] (brackets) matches characters or a character range separated by a hyphen.

Example [0137abcr-y] matches 0, 1, 3,v it does not match 2, 9, m, z

? (question mark) pattern matches zero or one instance. Entering Ctrl-V prior to the question mark prevents the CLI from interpreting ? as a help command.

Example x1?x matches xx and x1x

| (pipe) pattern matches character patterns on either side of bar.

Example B(E|A)D matches BED and BAD. It does not match BD, BEAD, BEED, or EAD

()(parenthesis) nests characters for matching. Endpoints of a range are separated with a dash (-).

Example 6(45)+ matches 645454523 it does not match 6443

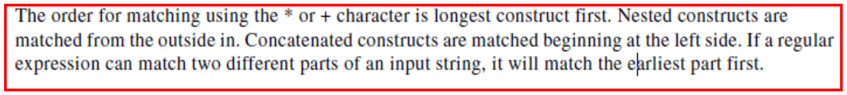
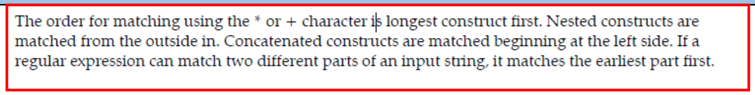
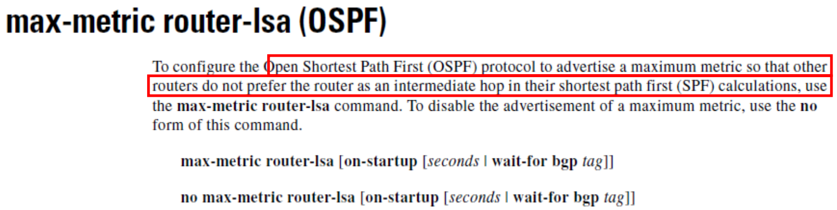
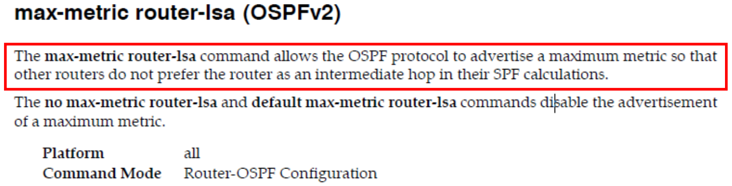
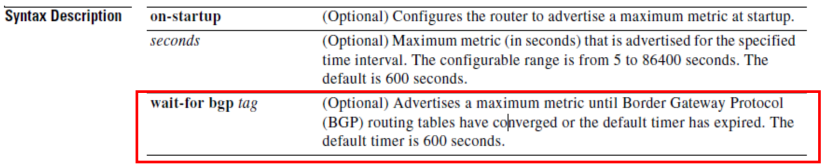
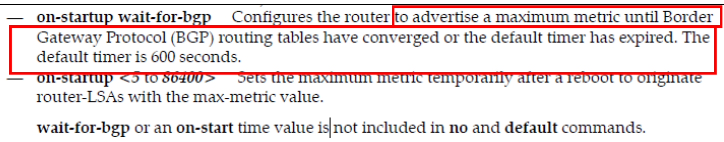
Example ([A-Za-z][0-9])+ matches C4 or x9

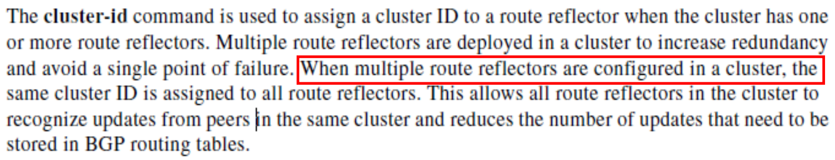
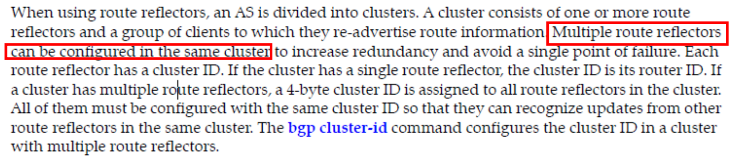
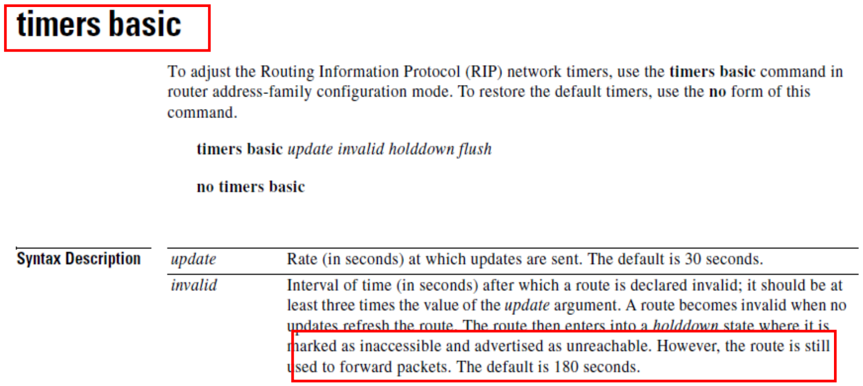
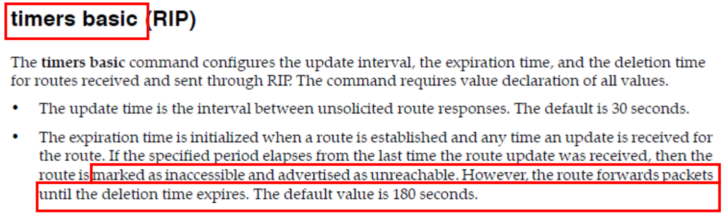
_ (underscore) Pattern replaces a long regular expression list by matching a comma (,), the beginning of the input string, the end of the input string, or a space.

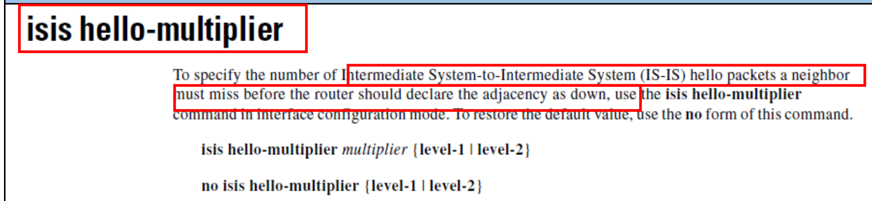
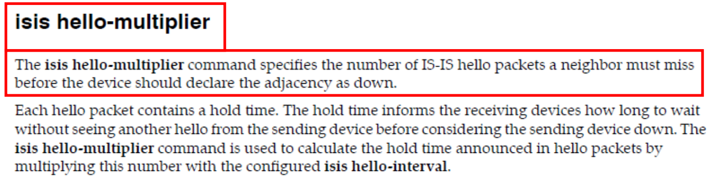
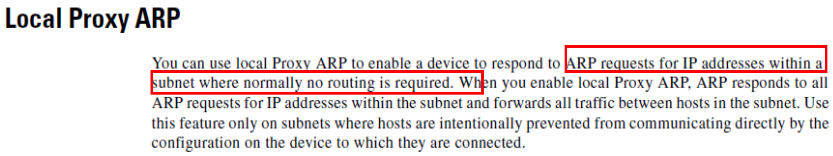
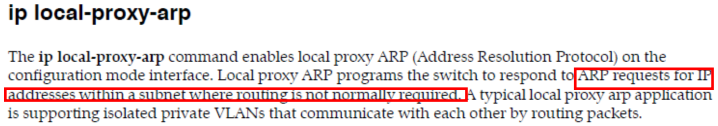
Example _rxy_ matches any of the following:

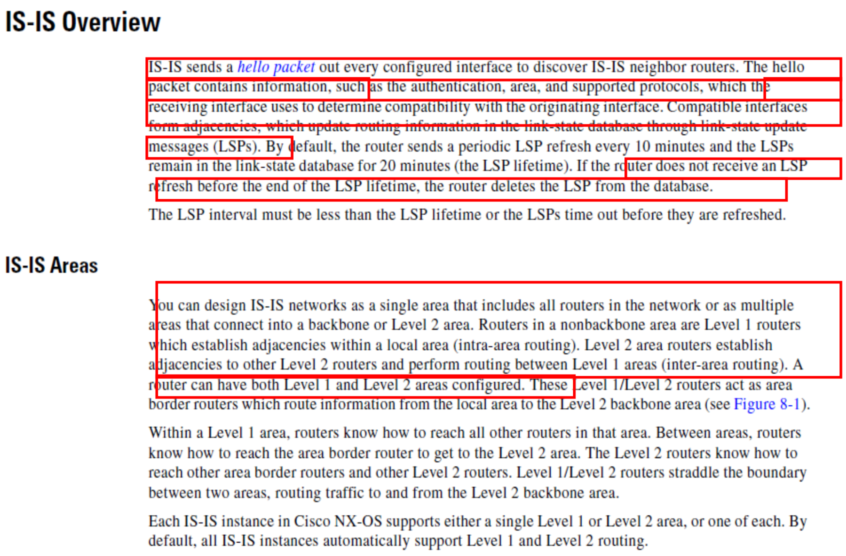
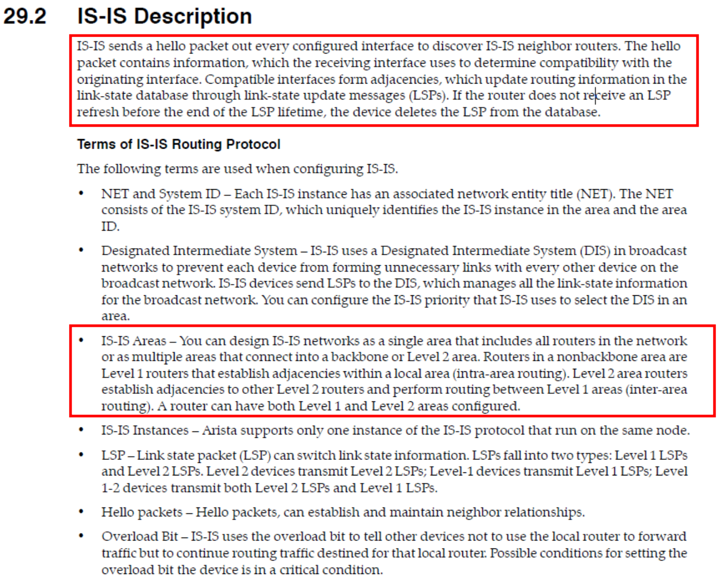
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 106.

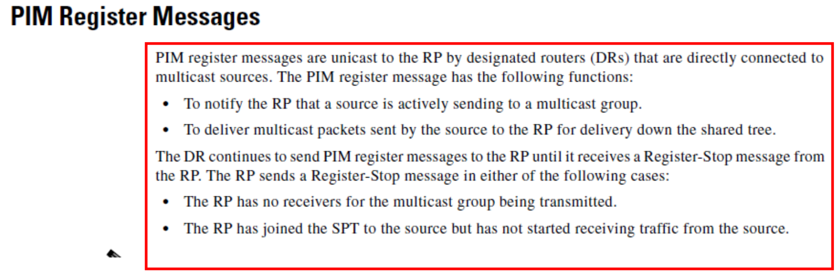
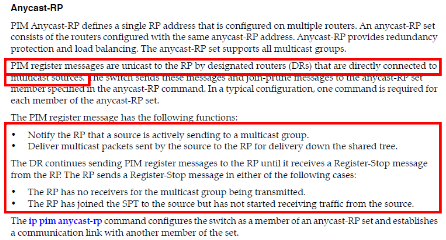
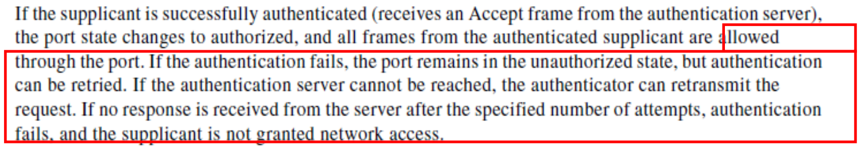
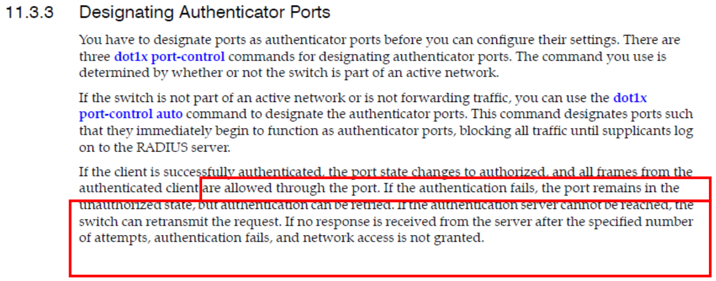
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 94; Arista User Manual, v. 4.11.1 (1/11/13), at 64; Arista User Manual v. 4.10.3 (10/22/12), at 56; Arista User Manual v. 4.9.3.2 (5/3/12), at 52; Arista User Manual v. 4.8.2 (11/18/11), at 48.
</td>
<td>Dkt. 419-10 at PDF p. 106</td>
</tr>
</table>

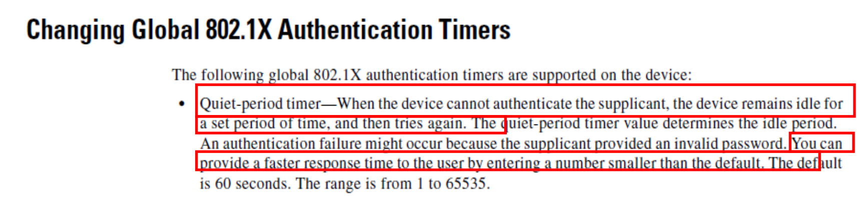
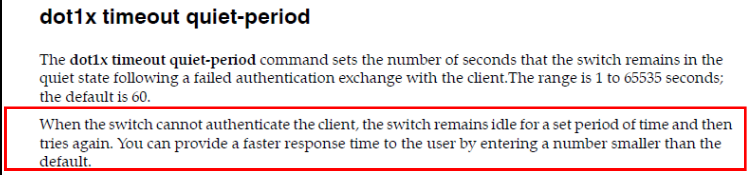
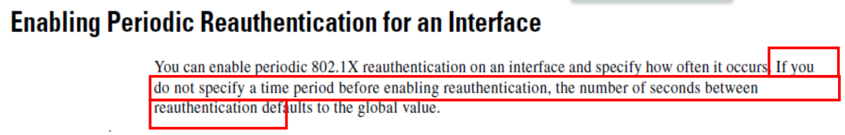
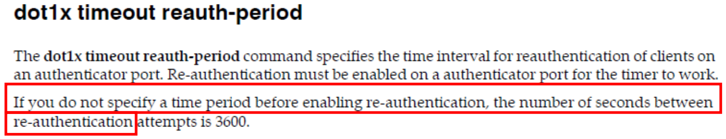
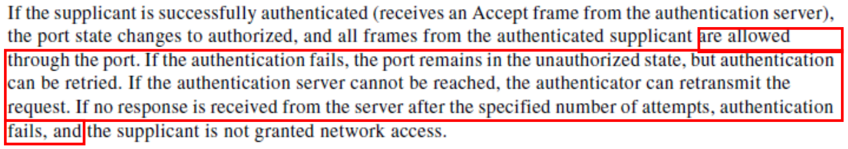
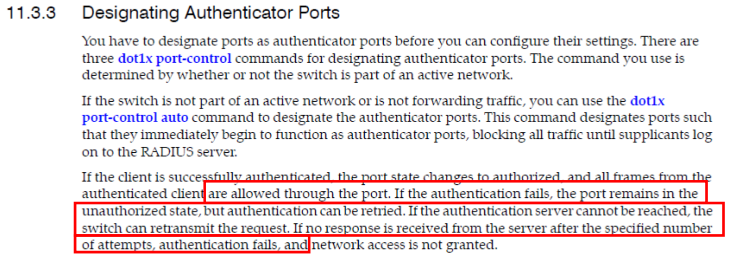
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at A-3.	 The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 107. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.	Dkt. 419-10 at PDF p. 107
 **max-metric router-lsa (OSPF)** To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command. To disable the advertisement of a maximum metric, use the **no** form of this command. **max-metric router-lsa** [**on-startup** [*seconds* | **wait-for bgp** *tag*]] **no max-metric router-lsa** [**on-startup** [*seconds* | **wait-for bgp** *tag*]] Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-272.	 **max-metric router-lsa (OSPFv2)** The **max-metric router-lsa** command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations. The **no max-metric router-lsa** and **default max-metric router-lsa** commands disable the advertisement of a maximum metric. **Platform** all **Command Mode** Router-OSPF Configuration Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1439.	Dkt. 419-10 at PDF p. 107
 **Syntax Description** **on-startup** (Optional) Configures the router to advertise a maximum metric at startup. *seconds* (Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds. **wait-for bgp** *tag* (Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-272.	 — **on-startup wait-for-bgp** Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. — **on-startup** *<5 to 86400>* Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value. **wait-for-bgp** or an **on-start** time value is not included in **no** and **default** commands. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1439.	Dkt. 419-10 at PDF p. 107

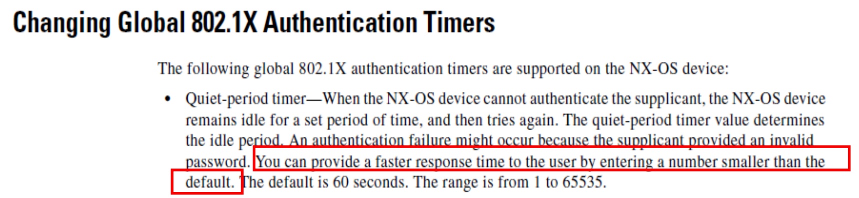
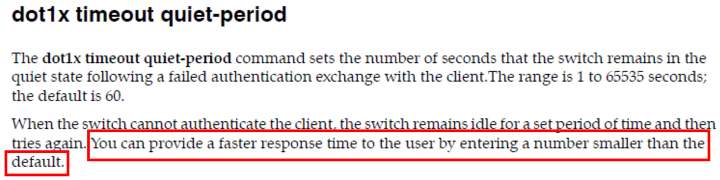
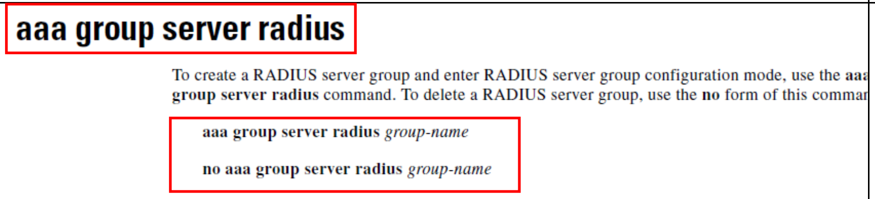
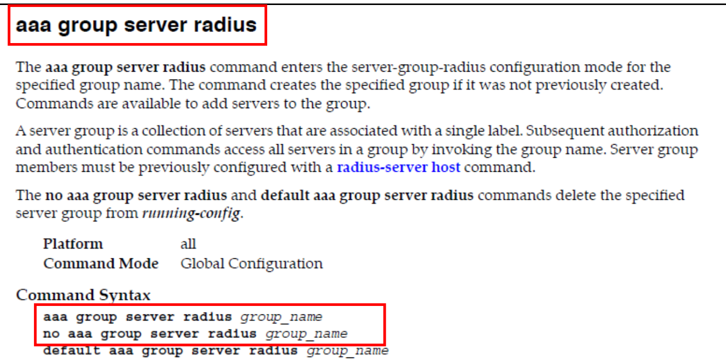
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 The **cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables. Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-564.	 When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The **bgp cluster-id** command configures the cluster ID in a cluster with multiple route reflectors. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1549. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.	Dkt. 419-10 at PDF p. 108
 **timers basic** To adjust the Routing Information Protocol (RIP) network timers, use the **timers basic** command in router address-family configuration mode. To restore the default timers, use the **no** form of this command. **timers basic** *update invalid holddown flush* **no timers basic** **Syntax Description** *update* Rate (in seconds) at which updates are sent. The default is 30 seconds. *invalid* Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when no updates refresh the route. The route then enters into a *holddown* state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds. Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-538.	 **timers basic (RIP)** The **timers basic** command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values. • The update time is the interval between unsolicited route responses. The default is 30 seconds. • The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1671. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 (11/18/11), at 570.	Dkt. 419-10 at PDF p. 108

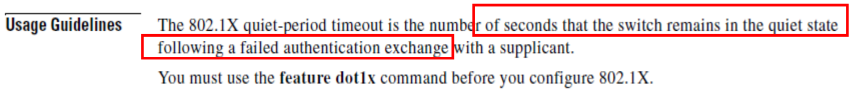
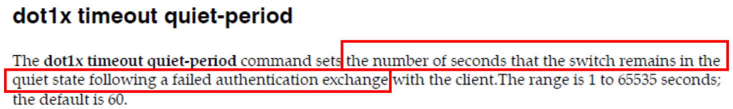
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **isis hello-multiplier** To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **isis hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command. **isis hello-multiplier** *multiplier* {**level-1** | **level-2**} **no isis hello-multiplier** {**level-1** | **level-2**} Cisco NX-OS Unicast Routing Command Reference (2008), Release 4.0, at L3-224.	 **isis hello-multiplier** The **isis hello-multiplier** command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down. Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The **isis hello-multiplier** command is used to calculate the hold time announced in hello packets by multiplying this number with the configured **isis hello-interval**. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1685. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1447.	Dkt. 419-10 at PDF p. 109
 **Local Proxy ARP** You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected. Cisco NX-OS Unicast Routing Configuration Guide (2008), Release 4.0, at 2-5.	 **ip local-proxy-arp** The **ip local-proxy-arp** command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1276. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 856; Arista User Manual v. 4.10.3 (10/22/12), at 707.	Dkt. 419-10 at PDF p. 109

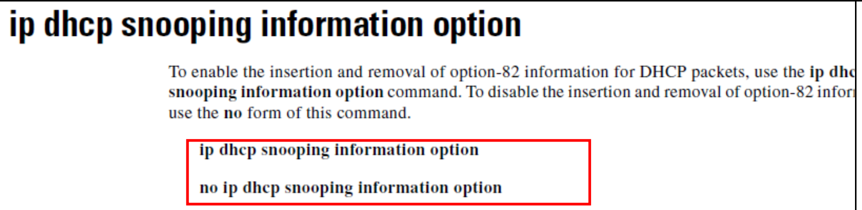
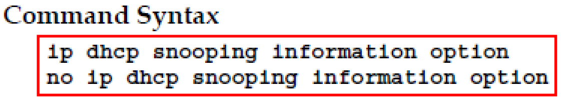
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **IS-IS Overview** IS-IS sends a *hello packet* out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database. The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed. **IS-IS Areas** You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers which establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers which route information from the local area to the Level 2 backbone area (see Figure 8-1). Within a Level 1 area, routers know how to reach all other routers in that area. Between areas, routers know how to reach the area border router to get to the Level 2 area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Each IS-IS instance in Cisco NX-OS supports either a single Level 1 or Level 2 area, or one of each. By default, all IS-IS instances automatically support Level 1 and Level 2 routing. Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0, at 8-2.	 **29.2 IS-IS Description** IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database. **Terms of IS-IS Routing Protocol** The following terms are used when configuring IS-IS. • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. • IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. • IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. • LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. • Hello packets – Hello packets, can establish and maintain neighbor relationships. • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1674. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1436.	Dkt. 419-10 at PDF p. 110

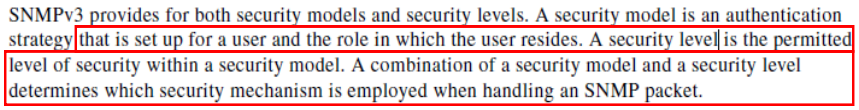
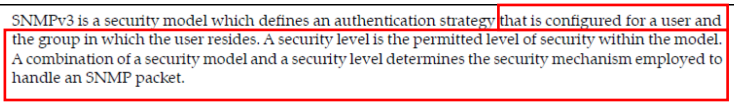
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **PIM Register Messages** PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions: • To notify the RP that a source is actively sending to a multicast group. • To deliver multicast packets sent by the source to the RP for delivery down the shared tree. The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases: • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. Cisco NX-OS Multicast Routing Configuration Guide (2008), Release 4.0, at 3-7.	 **Anycast-RP** PIM Anycast-RP defines a single RP address that is configured on multiple routers. An anycast-RP set consists of the routers configured with the same anycast-RP address. Anycast-RP provides redundancy protection and load balancing. The anycast-RP set supports all multicast groups. PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The switch sends these messages and join-prune messages to the anycast-RP set member specified in the anycast-RP command. In a typical configuration, one command is required for each member of the anycast-RP set. The PIM register message has the following functions: • Notify the RP that a source is actively sending to a multicast group. • Deliver multicast packets sent by the source to the RP for delivery down the shared tree. The DR continues sending PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases: • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. The ip pim anycast-rp command configures the switch as a member of an anycast-RP set and establishes a communication link with another member of the set. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1874. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1580; Arista User Manual, v. 4.11.1 (1/11/13), at 1274; Arista User Manual v. 4.10.3 (10/22/12), at 1005-06; Arista User Manual v. 4.9.3.2 (5/3/12), at 763-65; Arista User Manual v. 4.8.2 (11/18/11), at 639; Arista User Manual v. 4.7.3 (7/18/11), at 514.	Dkt. 419-10 at PDF p. 111
 If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access. Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-5.	 11.3.3 Designating Authenticator Ports You have to designate ports as authenticator ports before you can configure their settings. There are three dot1x port-control commands for designating authenticator ports. The command you use is determined by whether or not the switch is part of an active network. If the switch is not part of an active network or is not forwarding traffic, you can use the dot1x port-control auto command to designate the authenticator ports. This command designates ports such that they immediately begin to function as authenticator ports, blocking all traffic until supplicants log on to the RADIUS server. If the client is successfully authenticated, the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 558.	Dkt. 419-10 at PDF p. 111

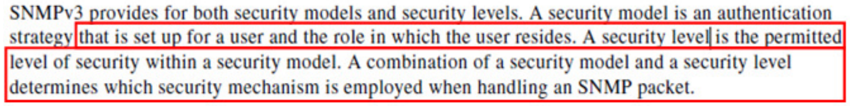
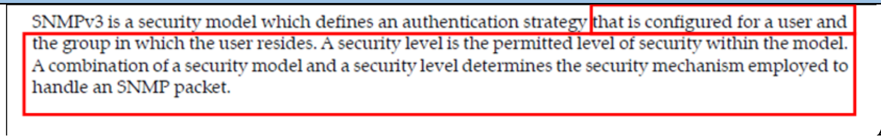
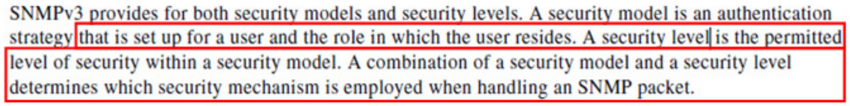
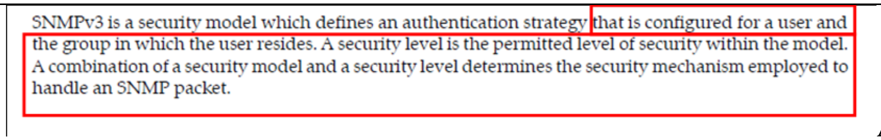
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Changing Global 802.1X Authentication Timers** The following global 802.1X authentication timers are supported on the device: • Quiet-period timer—When the device cannot authenticate the supplicant, the device remains idle for a set period of time, and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default. The default is 60 seconds. The range is from 1 to 65535. Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-14.	 **dot1x timeout quiet-period** The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60. When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 569.	Dkt. 419-10 at PDF p. 112
 **Enabling Periodic Reauthentication for an Interface** You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value. Cisco DCNM Security Configuration Guide (2008), Release 4.0, at 6-14	 **dot1x timeout reauth-period** The **dot1x timeout reauth-period** command specifies the time interval for reauthentication of clients on an authenticator port. Re-authentication must be enabled on a authenticator port for the timer to work. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 570.	Dkt. 419-10 at PDF p. 112
 If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access. Cisco NX-OS Security Configuration Guide (2008), Release 4.0, at 7-5.	 11.3.3 Designating Authenticator Ports You have to designate ports as authenticator ports before you can configure their settings. There are three **dot1x port-control** commands for designating authenticator ports. The command you use is determined by whether or not the switch is part of an active network. If the switch is not part of an active network or is not forwarding traffic, you can use the **dot1x port-control auto** command to designate the authenticator ports. This command designates ports such that they immediately begin to function as authenticator ports, blocking all traffic until supplicants log on to the RADIUS server. If the client is successfully authenticated, the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 558.	Dkt. 419-10 at PDF p. 112

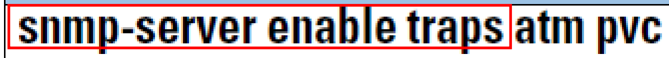
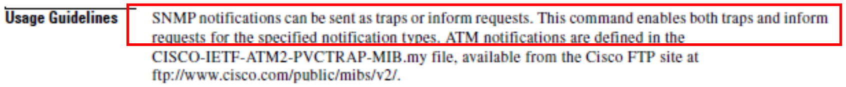
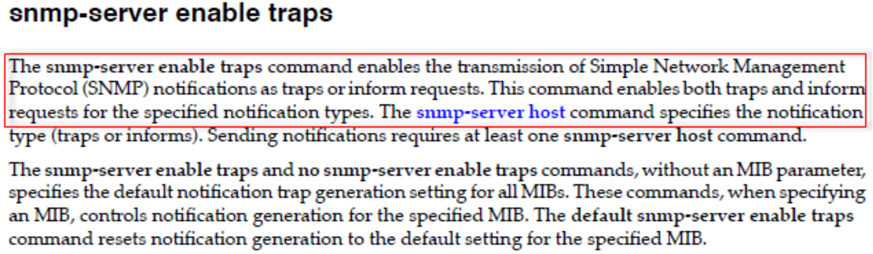
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Changing Global 802.1X Authentication Timers** The following global 802.1X authentication timers are supported on the NX-OS device: • Quiet-period timer—When the NX-OS device cannot authenticate the supplicant, the NX-OS device remains idle for a set period of time, and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default. The default is 60 seconds. The range is from 1 to 65535. Cisco NX-OS Security Configuration Guide (2008), Release 4.0, at 7-18.	 **dot1x timeout quiet-period** The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60. When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 569.	Dkt. 419-10 at PDF p. 113
 **aaa group server radius** To create a RADIUS server group and enter RADIUS server group configuration mode, use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this commar **aaa group server radius** *group-name* **no aaa group server radius** *group-name* Cisco NX-OS Security Command Reference (2008), Release 4.0, at 17.	 **aaa group server radius** The **aaa group server radius** command enters the server-group-radius configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group. A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a radius-server host command. The **no aaa group server radius** and **default aaa group server radius** commands delete the specified server group from *running-config*. **Platform** all **Command Mode** Global Configuration Command Syntax `aaa group server radius` *group_name* `no aaa group server radius` *group_name* `default aaa group server radius` *group_name* Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 224. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 217; Arista User Manual, v. 4.11.1 (1/11/13), at 126; Arista User Manual v. 4.12.3 (7/17/13), at 168; Arista User Manual v. 4.10.3 (10/22/12), at 118.	Dkt. 419-10 at PDF p. 113

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Usage Guidelines** The 802.1X quiet-period timeout is the number of seconds that the switch remains in the quiet state following a failed authentication exchange with a supplicant. You must use the **feature dot1x** command before you configure 802.1X. Cisco NX-OS Security Command Reference (2008), Release 4.0, at 119.	 **dot1x timeout quiet-period** The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 569.	Dkt. 419-10 at PDF p. 114

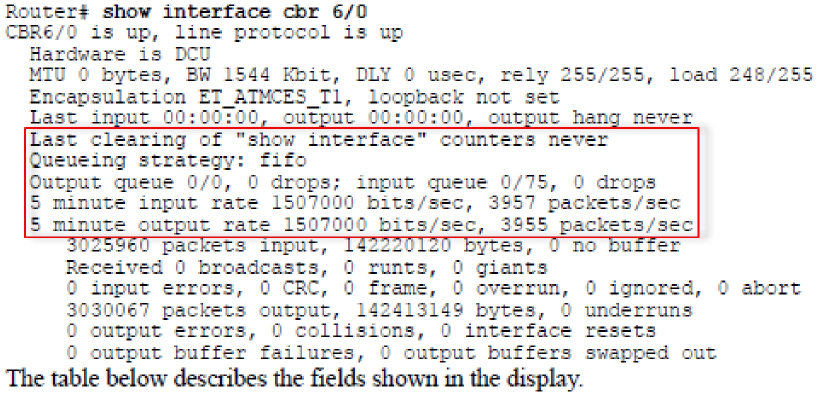

ip dhcp snooping information option
To enable the insertion and removal of option-82 information for DHCP packets, use the **ip dhc snooping information option** command. To disable the insertion and removal of option-82 infor use the **no** form of this command.
ip dhcp snooping information option
no ip dhcp snooping information option
Cisco NX-OS Security Command Reference (2008), Release 4.0, at 196.
	
	Command Syntax
	`ip dhcp snooping information option`
	`no ip dhcp snooping information option`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1270.
		Dkt. 419-10 at PDF p. 114

 SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco NX-OS System Management Configuration Guide (2008), Release 4.0, at 7-2,	 SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1964. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 114

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco NX-OS System Management Configuration Guide (2010), Release 5.0, at 10-2.	 SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. A rista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1964. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 115
 SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Configuring SNMP Support (2008), at 17.	 SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. A rista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1964. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1342; Arista User Manual v. 4.10.3 (10/22/12), at 1108; Arista User Manual v. 4.9.3.2 (5/3/12), at 864; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 115

Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record
 **snmp-server enable traps atm pvc** …  **Usage Guidelines** SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/. Cisco IOS Asynchronous Transfer Mode Command Reference (2013), at 526.	 **snmp-server enable traps** The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command. The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1990. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.	Dkt. 419-10 at PDF p. 116

<table>
<tr><th>Cisco’s Documentation</th><th>Arista’s Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

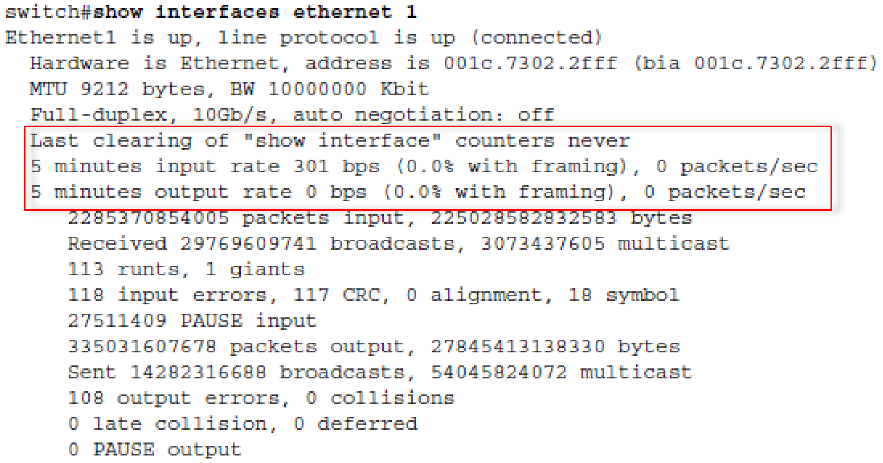


```
Router# show interface cbr 6/0
CBR6/0 is up, line protocol is up
  Hardware is DCU
  MTU 0 bytes, BW 1544 Kbit, DLY 0 usec, rely 255/255, load 248/255
  Encapsulation ET_ATMCES_T1, loopback not set
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1507000 bits/sec, 3957 packets/sec
  5 minute output rate 1507000 bits/sec, 3955 packets/sec
     3025960 packets input, 142220120 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3030067 packets output, 142413149 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the fields shown in the display.

Cisco IOS Asynchronous Transfer Mode Command Reference (2013), at 460.

</td>
<td>

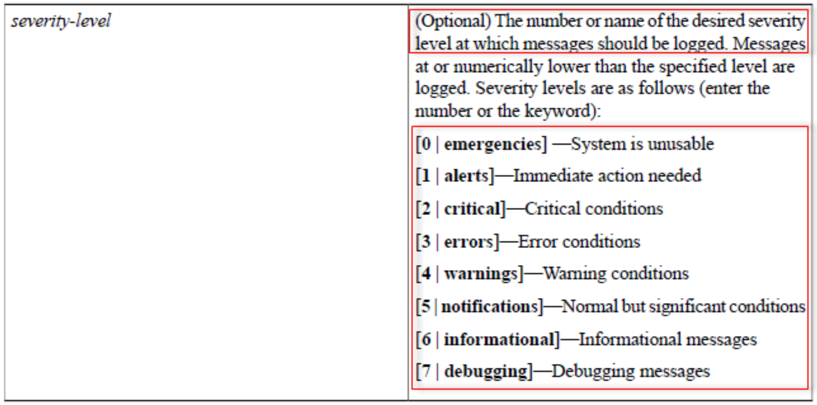
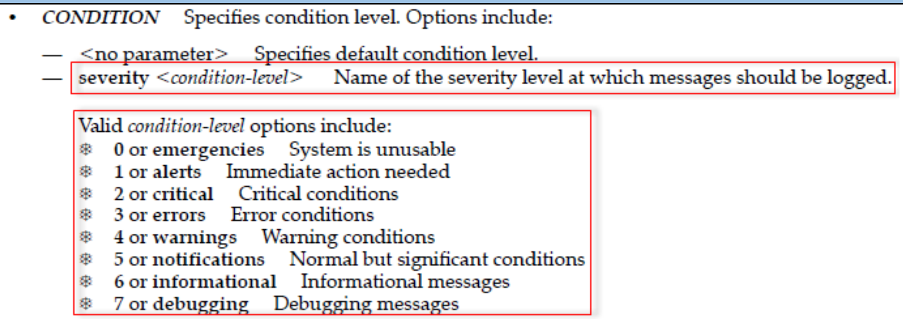
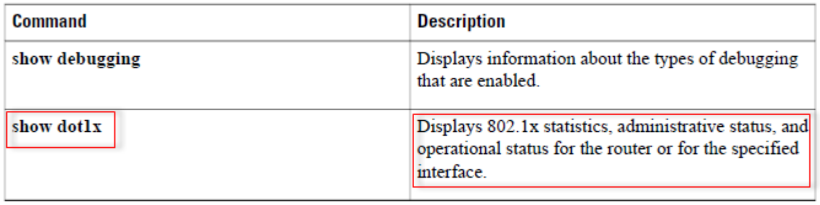
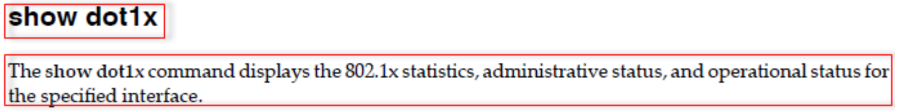


```
switch#show interfaces ethernet 1
Ethernet1 is up, line protocol is up (connected)
  Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff)
  MTU 9212 bytes, BW 10000000 Kbit
  Full-duplex, 10Gb/s, auto negotiation: off
  Last clearing of "show interface" counters never
  5 minutes input rate 301 bps (0.0% with framing), 0 packets/sec
  5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec
     2285370854005 packets input, 225028582832583 bytes
     Received 29769609741 broadcasts, 3073437605 multicast
     113 runts, 1 giants
     118 input errors, 117 CRC, 0 alignment, 18 symbol
     27511409 PAUSE input
     335031607678 packets output, 27845413138330 bytes
     Sent 14282316688 broadcasts, 54045824072 multicast
     108 output errors, 0 collisions
     0 late collision, 0 deferred
     0 PAUSE output
```

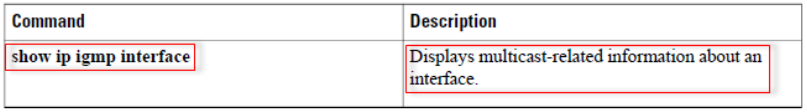
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 437.

See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.

</td>
<td>Dkt. 419-10 at PDF p. 117</td>
</tr>
</table>

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>
<i>severity-level</i> (Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):
[0 | <b>emergencies</b>] —System is unusable
[1 | <b>alerts</b>]—Immediate action needed
[2 | <b>critical</b>]—Critical conditions
[3 | <b>errors</b>]—Error conditions
[4 | <b>warnings</b>]—Warning conditions
[5 | <b>notifications</b>]—Normal but significant conditions
[6 | <b>informational</b>]—Informational messages
[7 | <b>debugging</b>]—Debugging messages
Cisco IOS Cisco Networking Services Command Reference (2013), at 91.</td>
<td>
• <i>CONDITION</i> Specifies condition level. Options include:
— &lt;no parameter&gt; Specifies default condition level.
— severity &lt;<i>condition-level</i>&gt; Name of the severity level at which messages should be logged.
Valid <i>condition-level</i> options include:
- 0 or emergencies System is unusable
- 1 or alerts Immediate action needed
- 2 or critical Critical conditions
- 3 or errors Error conditions
- 4 or warnings Warning conditions
- 5 or notifications Normal but significant conditions
- 6 or informational Informational messages
- 7 or debugging Debugging messages
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 155.</td>
<td>Dkt. 419-10 at PDF p. 118</td>
</tr>
<tr>
<td>
<b>Command</b> | <b>Description</b>
<b>show debugging</b> Displays information about the types of debugging that are enabled.
<b>show dot1x</b> Displays 802.1x statistics, administrative status, and operational status for the router or for the specified interface.
Cisco IOS Debug Command Reference – Commands A through D (2013), at 635.</td>
<td>
<b>show dot1x</b>
The show dot1x command displays the 802.1x statistics, administrative status, and operational status for the specified interface.
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 572.</td>
<td>Dkt. 419-10 at PDF p. 118</td>
</tr>
</table>

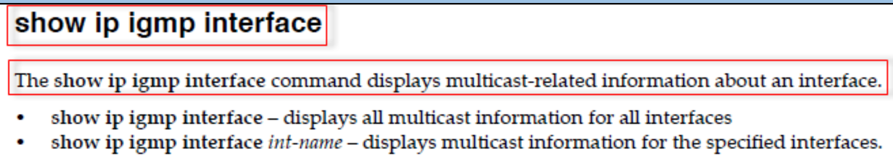
<table>
<tr>
<th>Cisco's Documentation</th>
<th>Arista's Documentation</th>
<th>Supporting Evidence In The Record</th>
</tr>
<tr>
<td>



<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>show ip igmp interface</td><td>Displays multicast-related information about an interface.</td></tr>
</table>

Cisco IOS Debug Command Reference – Commands I through L (2013), at 297.

</td>
<td>



show ip igmp interface

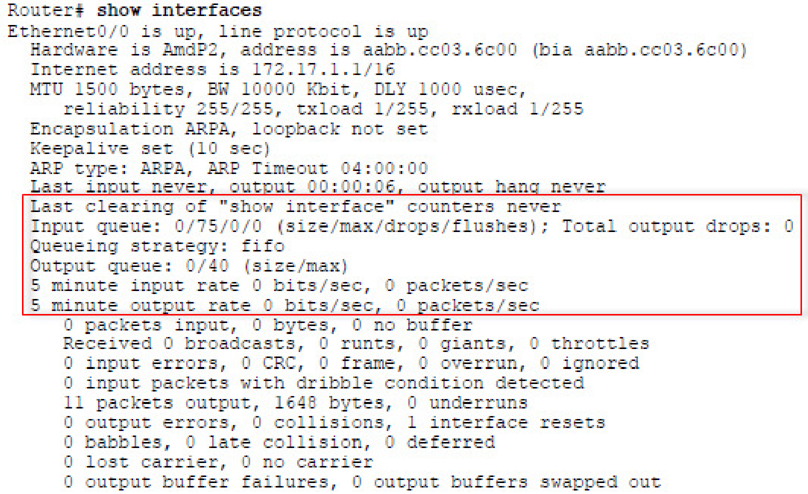
The show ip igmp interface command displays multicast-related information about an interface.

- **show ip igmp interface** – displays all multicast information for all interfaces
- **show ip igmp interface** *int-name* – displays multicast information for the specified interfaces.

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1850.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.

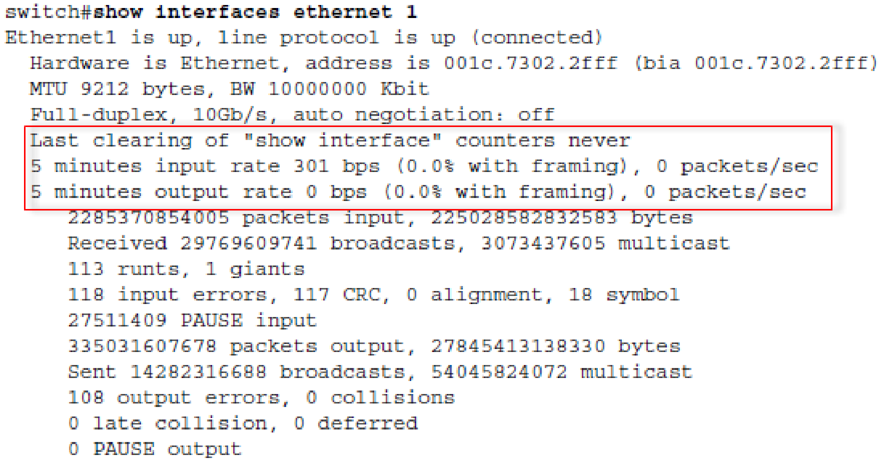
</td>
<td>Dkt. 419-10 at PDF p. 119</td>
</tr>
<tr>
<td>



```
Router# show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc03.6c00 (bia aabb.cc03.6c00)
  Internet address is 172.17.1.1/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     11 packets output, 1648 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Cisco Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T (2013), at 44.

</td>
<td>

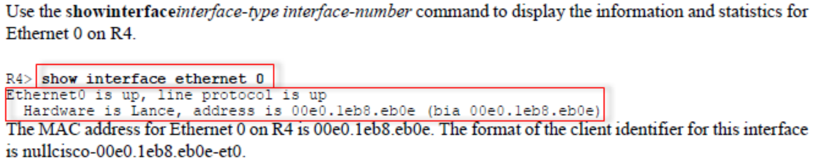


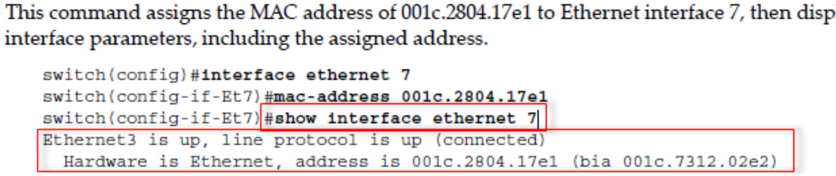
```
switch#show interfaces ethernet 1
Ethernet1 is up, line protocol is up (connected)
  Hardware is Ethernet, address is 001c.7302.2fff (bia 001c.7302.2fff)
  MTU 9212 bytes, BW 10000000 Kbit
  Full-duplex, 10Gb/s, auto negotiation: off
  Last clearing of "show interface" counters never
  5 minutes input rate 301 bps (0.0% with framing), 0 packets/sec
  5 minutes output rate 0 bps (0.0% with framing), 0 packets/sec
     2285370854005 packets input, 225028582832583 bytes
     Received 29769609741 broadcasts, 3073437605 multicast
     113 runts, 1 giants
     118 input errors, 117 CRC, 0 alignment, 18 symbol
     27511409 PAUSE input
     335031607678 packets output, 27845413138330 bytes
     Sent 14282316688 broadcasts, 54045824072 multicast
     108 output errors, 0 collisions
     0 late collision, 0 deferred
     0 PAUSE output
```

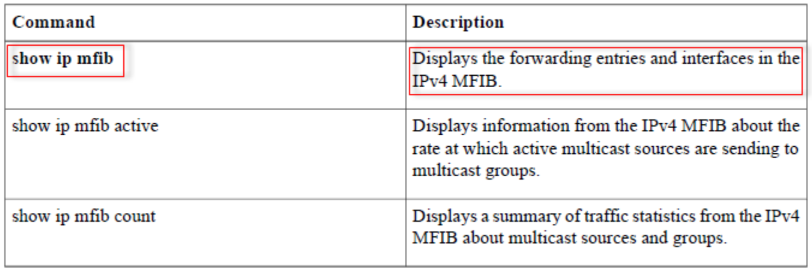
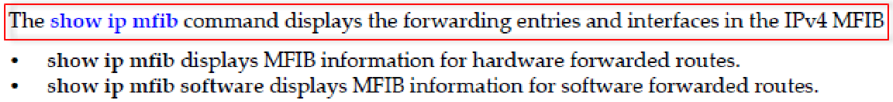
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 437.

See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.

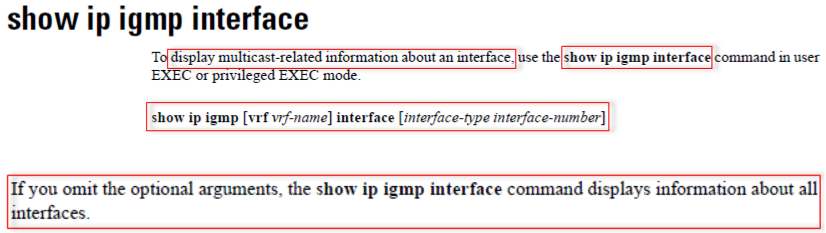
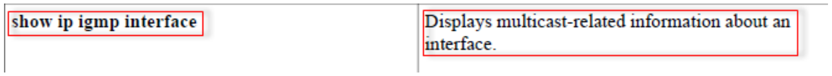
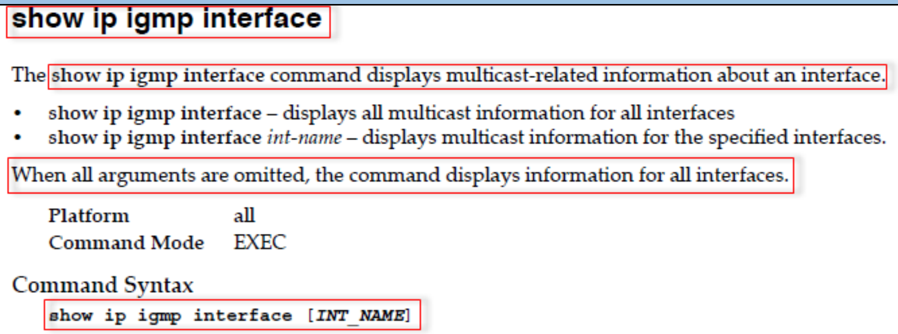
</td>
<td>Dkt. 419-10 at PDF p. 119</td>
</tr>
</table>

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

Use the <b>showinterface</b><i>interface-type interface-number</i> command to display the information and statistics for Ethernet 0 on R4.
<pre>
R4> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb0e (bia 00e0.1eb8.eb0e)
</pre>
The MAC address for Ethernet 0 on R4 is 00e0.1eb8.eb0e. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb0e-et0.

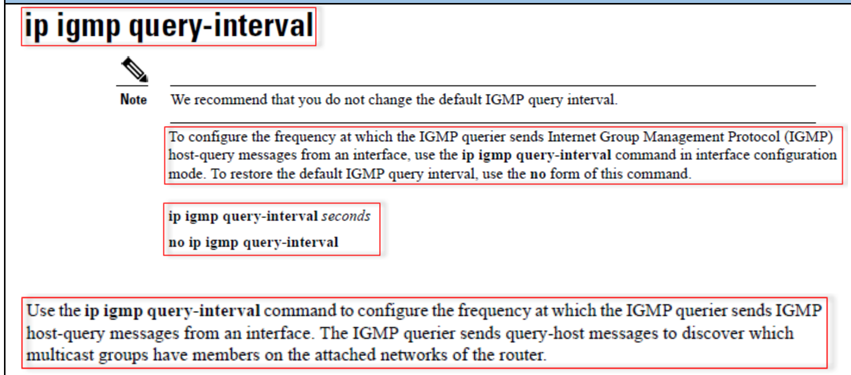
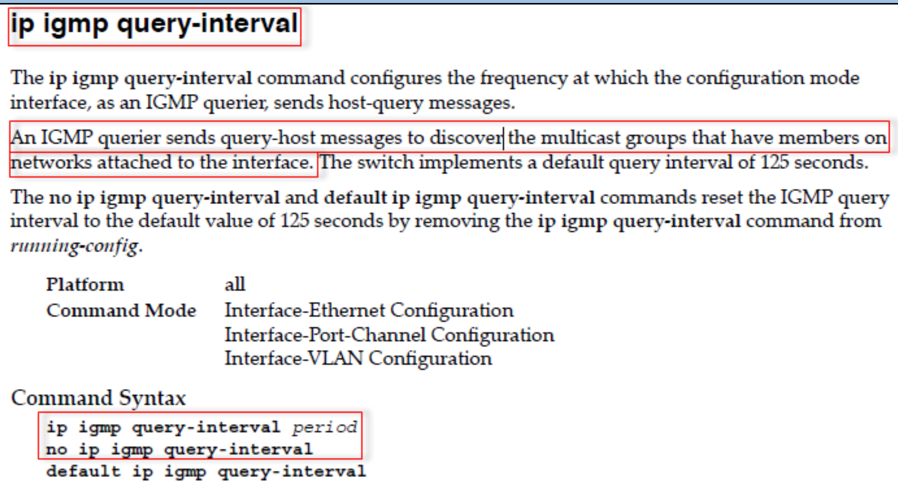
Cisco Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T (2013), at 81.
</td>
<td>

This command assigns the MAC address of 001c.2804.17e1 to Ethernet interface 7, then displays interface parameters, including the assigned address.
<pre>
    switch(config)#interface ethernet 7
    switch(config-if-Et7)#mac-address 001c.2804.17e1
    switch(config-if-Et7)#show interface ethernet 7
    Ethernet3 is up, line protocol is up (connected)
      Hardware is Ethernet, address is 001c.2804.17e1 (bia 001c.7312.02e2)
</pre>
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 437.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.
</td>
<td>Dkt. 419-10 at PDF p. 120</td>
</tr>
<tr>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>show ip mfib</b></td><td>Displays the forwarding entries and interfaces in the IPv4 MFIB.</td></tr>
<tr><td>show ip mfib active</td><td>Displays information from the IPv4 MFIB about the rate at which active multicast sources are sending to multicast groups.</td></tr>
<tr><td>show ip mfib count</td><td>Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups.</td></tr>
</table>
Cisco IOS Multicast Command Reference (2013), at 17.
</td>
<td>

The show ip mfib command displays the forwarding entries and interfaces in the IPv4 MFIB
<ul>
<li><b>show ip mfib</b> displays MFIB information for hardware forwarded routes.</li>
<li><b>show ip mfib software</b> displays MFIB information for software forwarded routes.</li>
</ul>
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1755.

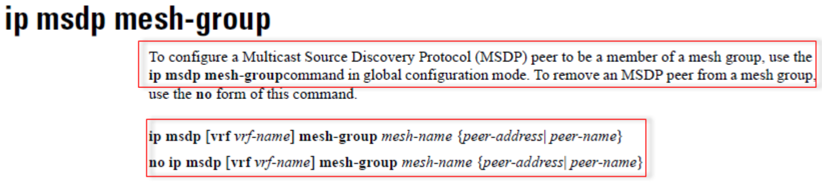
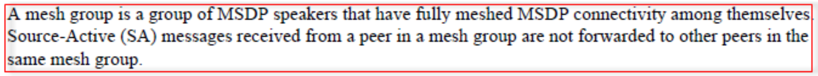
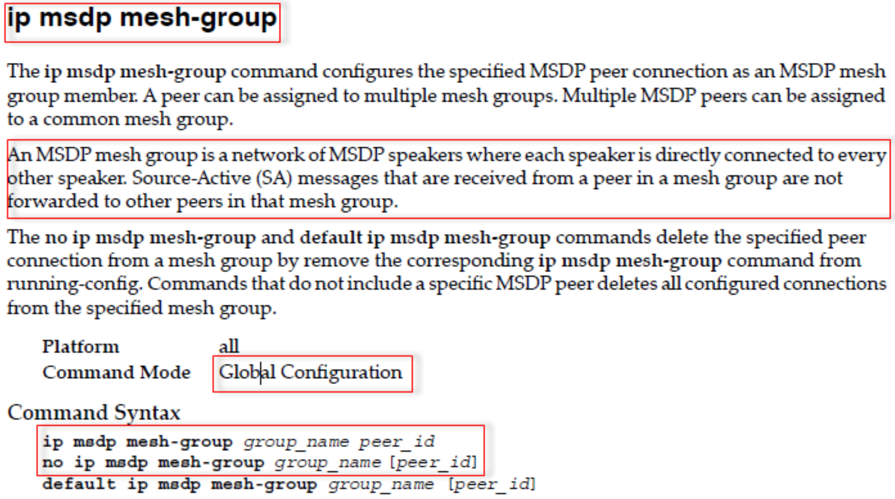
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1484; Arista User Manual, v. 4.11.1 (1/11/13), at 1186; Arista User Manual v. 4.10.3 (10/22/12), at 1020; Arista User Manual v. 4.9.3.2 (5/3/12), at 778; Arista User Manual v. 4.8.2 (11/18/11), at 597; Arista User Manual v. 4.7.3 (7/18/11), at 477; Arista User Manual v. 4.6.0 (12/22/2010), at 324.
</td>
<td>Dkt. 419-10 at PDF p. 120</td>
</tr>
</table>

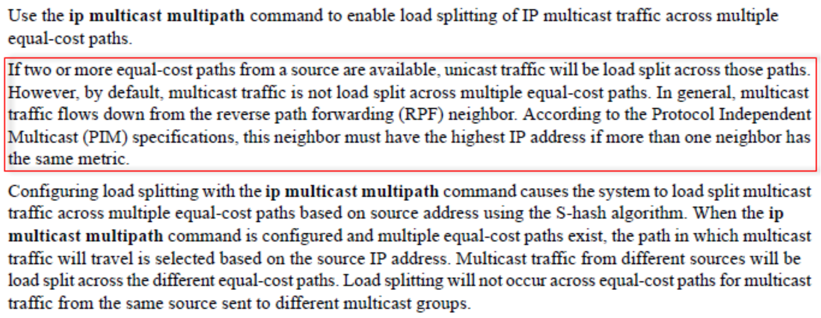
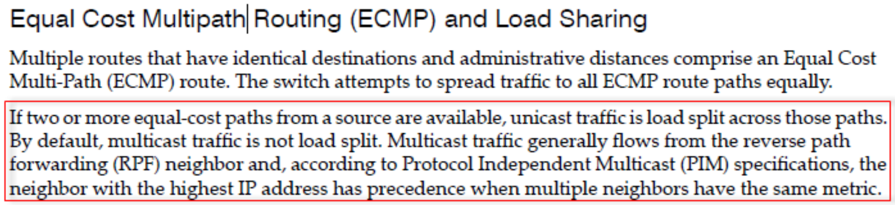
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **show ip igmp interface** To display multicast-related information about an interface, use the **show ip igmp interface** command in user EXEC or privileged EXEC mode. **show ip igmp** [**vrf** *vrf-name*] **interface** [*interface-type interface-number*] If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces. Cisco IOS Multicast Command Reference at 618 (2013)  **show ip igmp interface** Displays multicast-related information about an interface. Cisco IOS Multicast Command Reference (2013), at 12.	 **show ip igmp interface** The show ip igmp interface command displays multicast-related information about an interface. • show ip igmp interface – displays all multicast information for all interfaces • show ip igmp interface *int-name* – displays multicast information for the specified interfaces. When all arguments are omitted, the command displays information for all interfaces. Platform all Command Mode EXEC Command Syntax `show ip igmp interface [INT_NAME]` Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1850. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.	Dkt. 419-10 at PDF p. 121

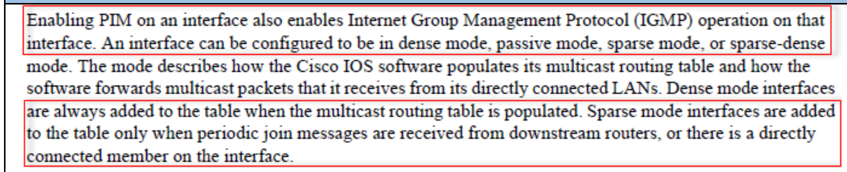
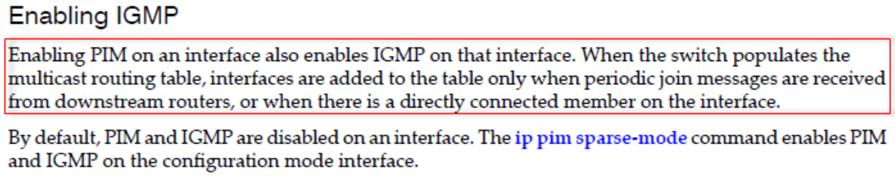
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


ip igmp query-interval
Note We recommend that you do not change the default IGMP query interval.
To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the **ip igmp query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.
ip igmp query-interval *seconds*
no ip igmp query-interval
Use the **ip igmp query-interval** command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.
Cisco IOS Multicast Command Reference (2013), at 118.
	
	ip igmp query-interval
	The **ip igmp query-interval** command configures the frequency at which the configuration mode interface, as an IGMP querier, sends host-query messages.
	An IGMP querier sends query-host messages to discover the multicast groups that have members on networks attached to the interface. The switch implements a default query interval of 125 seconds.
	The **no ip igmp query-interval** and **default ip igmp query-interval** commands reset the IGMP query interval to the default value of 125 seconds by removing the **ip igmp query-interval** command from *running-config*.
	Platform all
	Command Mode Interface-Ethernet Configuration
	Interface-Port-Channel Configuration
	Interface-VLAN Configuration
	Command Syntax
	`ip igmp query-interval` *`period`*
	`no ip igmp query-interval`
	`default ip igmp query-interval`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1802.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 1522; Arista User Manual, v. 4.11.1 (1/11/13), at 1219; Arista User Manual v. 4.10.3 (10/22/12), at 1028; Arista User Manual v. 4.9.3.2 (5/3/12), at 786; Arista User Manual v. 4.8.2 (11/18/11), at 605; Arista User Manual v. 4.7.3 (7/18/11), at 485; Arista User Manual v. 4.6.0 (12/22/2010), at 331.
		Dkt. 419-10 at PDF p. 122

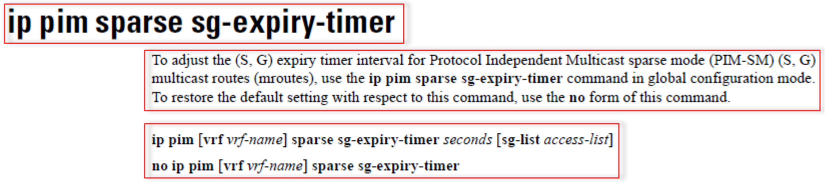
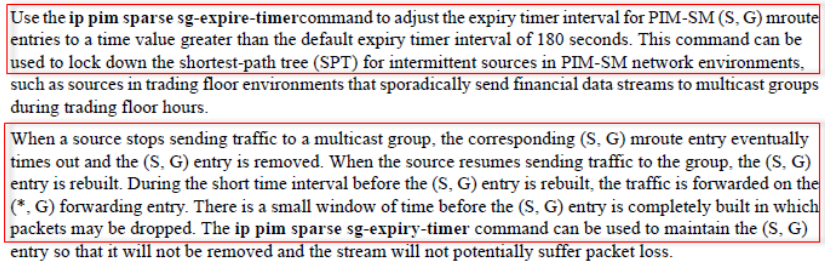
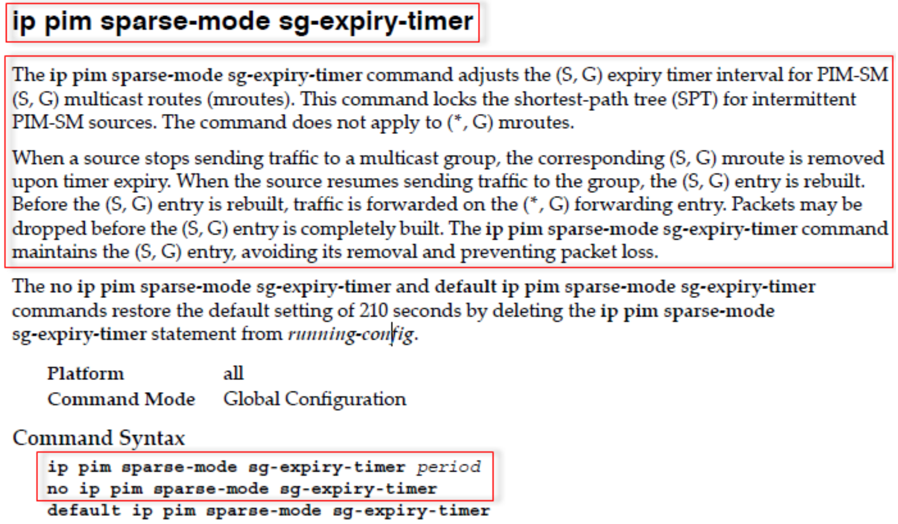
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record

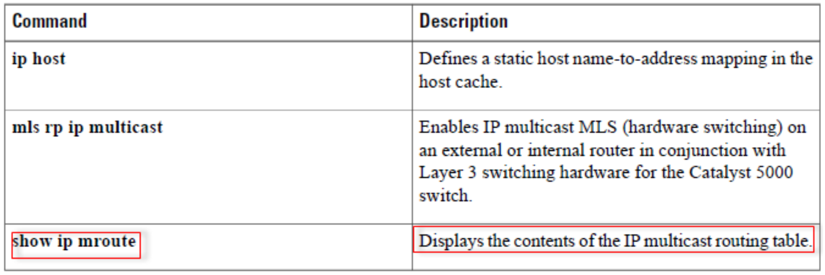
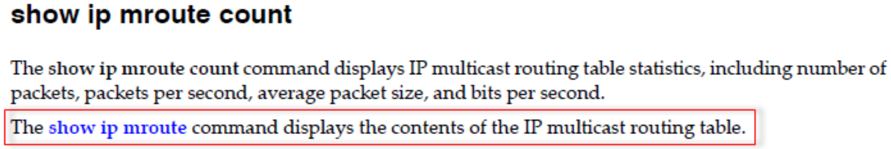

ip msdp mesh-group
To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group**command in global configuration mode. To remove an MSDP peer from a mesh group, use the **no** form of this command.
ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address*| *peer-name*}
no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address*| *peer-name*}
Cisco IOS Multicast Command Reference (2013), at 225

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.
Cisco IOS Multicast Command Reference (2013), at 226.
	
	ip msdp mesh-group
	The **ip msdp mesh-group** command configures the specified MSDP peer connection as an MSDP mesh group member. A peer can be assigned to multiple mesh groups. Multiple MSDP peers can be assigned to a common mesh group.
	An MSDP mesh group is a network of MSDP speakers where each speaker is directly connected to every other speaker. Source-Active (SA) messages that are received from a peer in a mesh group are not forwarded to other peers in that mesh group.
	The **no ip msdp mesh-group** and **default ip msdp mesh-group** commands delete the specified peer connection from a mesh group by remove the corresponding **ip msdp mesh-group** command from running-config. Commands that do not include a specific MSDP peer deletes all configured connections from the specified mesh group.
	Platform all
	Command Mode Global Configuration
	Command Syntax
	`ip msdp mesh-group group_name peer_id`
	`no ip msdp mesh-group group_name [peer_id]`
	`default ip msdp mesh-group group_name [peer_id]`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1928.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 1634; Arista User Manual, v. 4.11.1 (1/11/13), at 1325.
		Dkt. 419-10 at PDF p. 123

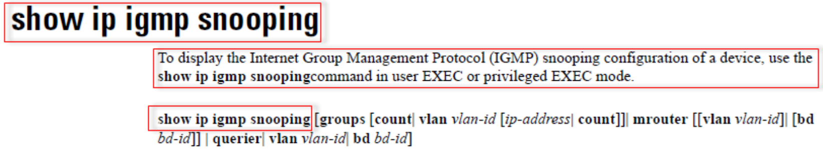
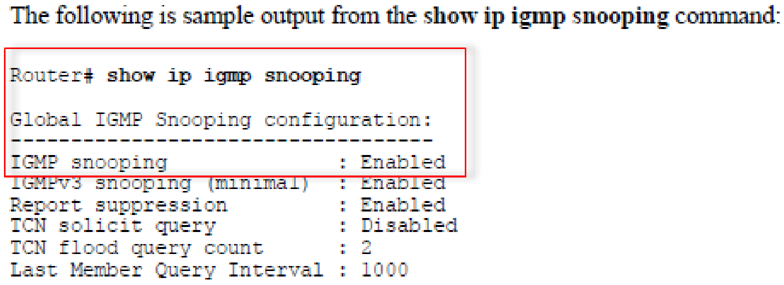
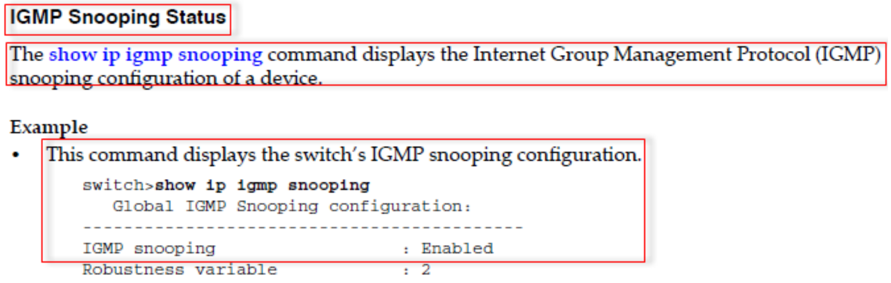
 Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths. If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric. Configuring load splitting with the **ip multicast multipath** command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups. Cisco IOS Multicast Command Reference (2013), at 284.	 Equal Cost Multipath Routing (ECMP) and Load Sharing Multiple routes that have identical destinations and administrative distances comprise an Equal Cost Multi-Path (ECMP) route. The switch attempts to spread traffic to all ECMP route paths equally. If two or more equal-cost paths from a source are available, unicast traffic is load split across those paths. By default, multicast traffic is not load split. Multicast traffic generally flows from the reverse path forwarding (RPF) neighbor and, according to Protocol Independent Multicast (PIM) specifications, the neighbor with the highest IP address has precedence when multiple neighbors have the same metric. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1231. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1191; Arista User Manual v. 4.12.3 (7/17/13), at 1042; Arista User Manual, v. 4.11.1 (1/11/13), at 398; Arista User Manual v. 4.10.3 (10/22/12), at 330.	Dkt. 419-10 at PDF p. 123

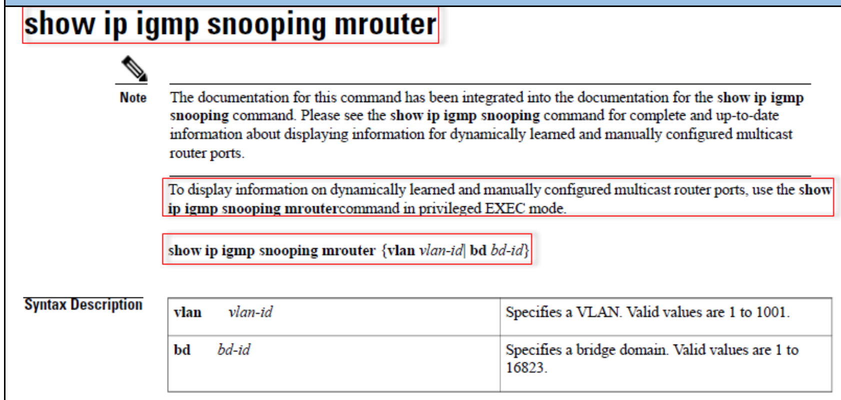
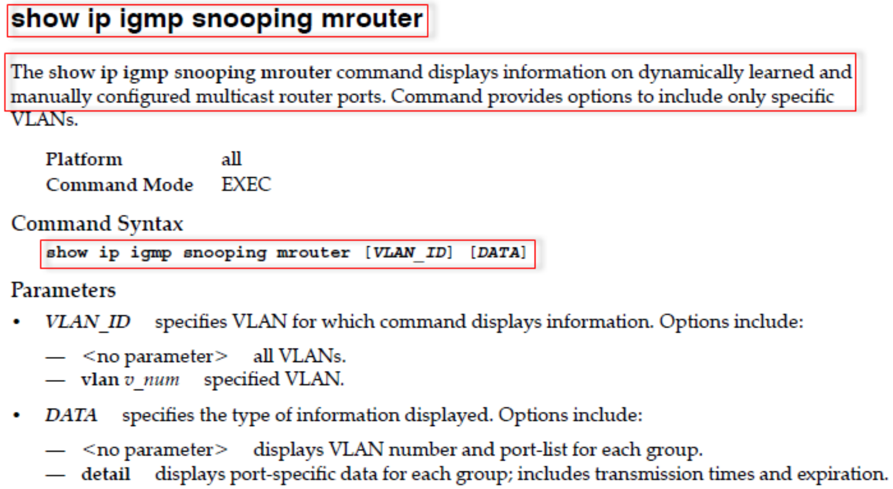
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets that it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface. Cisco IOS Multicast Command Reference (2013), at 330.	 Enabling IGMP Enabling PIM on an interface also enables IGMP on that interface. When the switch populates the multicast routing table, interfaces are added to the table only when periodic join messages are received from downstream routers, or when there is a directly connected member on the interface. By default, PIM and IGMP are disabled on an interface. The ip pim sparse-mode command enables PIM and IGMP on the configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1778. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1726; Arista User Manual v. 4.12.3 (7/17/13), at 1504; Arista User Manual, v. 4.11.1 (1/11/13), at 1204; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 at 578; Arista User Manual v. 4.7.3 (7/18/11), at 458; Arista User Manual v. 4.6.0 (12/22/2010), at 308.	Dkt. 419-10 at PDF p. 124

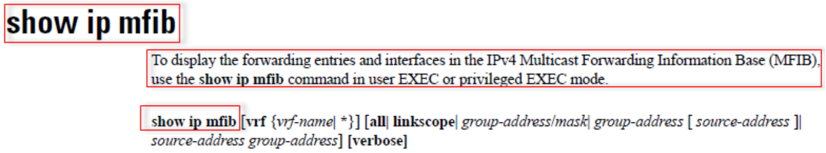
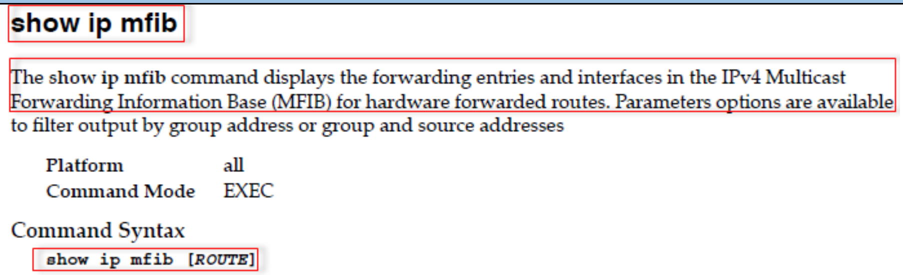
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


ip pim sparse sg-expiry-timer
To adjust the (S, G) expiry timer interval for Protocol Independent Multicast sparse mode (PIM-SM) (S, G) multicast routes (mroutes), use the **ip pim sparse sg-expiry-timer** command in global configuration mode. To restore the default setting with respect to this command, use the **no** form of this command.
ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer** *seconds* [**sg-list** *access-list*]
no ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer**
Cisco IOS Multicast Command Reference (2013), at 405.

Use the **ip pim sparse sg-expire-timer**command to adjust the expiry timer interval for PIM-SM (S, G) mroute entries to a time value greater than the default expiry timer interval of 180 seconds. This command can be used to lock down the shortest-path tree (SPT) for intermittent sources in PIM-SM network environments, such as sources in trading floor environments that sporadically send financial data streams to multicast groups during trading floor hours.
When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute entry eventually times out and the (S, G) entry is removed. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. During the short time interval before the (S, G) entry is rebuilt, the traffic is forwarded on the (*, G) forwarding entry. There is a small window of time before the (S, G) entry is completely built in which packets may be dropped. The **ip pim sparse sg-expiry-timer** command can be used to maintain the (S, G) entry so that it will not be removed and the stream will not potentially suffer packet loss.
Cisco IOS Multicast Command Reference(2013), at 406.
	
	ip pim sparse-mode sg-expiry-timer
	The **ip pim sparse-mode sg-expiry-timer** command adjusts the (S, G) expiry timer interval for PIM-SM (S, G) multicast routes (mroutes). This command locks the shortest-path tree (SPT) for intermittent PIM-SM sources. The command does not apply to (*, G) mroutes.
	When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute is removed upon timer expiry. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. Before the (S, G) entry is rebuilt, traffic is forwarded on the (*, G) forwarding entry. Packets may be dropped before the (S, G) entry is completely built. The **ip pim sparse-mode sg-expiry-timer** command maintains the (S, G) entry, avoiding its removal and preventing packet loss.
	The **no ip pim sparse-mode sg-expiry-timer** and **default ip pim sparse-mode sg-expiry-timer** commands restore the default setting of 210 seconds by deleting the **ip pim sparse-mode sg-expiry-timer** statement from *running-config*.
	Platform all
	Command Mode Global Configuration
	Command Syntax
	`ip pim sparse-mode sg-expiry-timer period`
	`no ip pim sparse-mode sg-expiry-timer`
	`default ip pim sparse-mode sg-expiry-timer`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1896.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 1602; Arista User Manual, v. 4.11.1 (1/11/13), at 1297; Arista User Manual v. 4.10.3 (10/22/12), at 1091; Arista User Manual v. 4.9.3.2 (5/3/12), at 848; Arista User Manual v. 4.8.2 (11/18/11), at 646; Arista User Manual v. 4.7.3 (7/18/11), at 516; Arista User Manual v. 4.6.0 (12/22/2010), at 361.
		Dkt. 419-10 at PDF p. 125

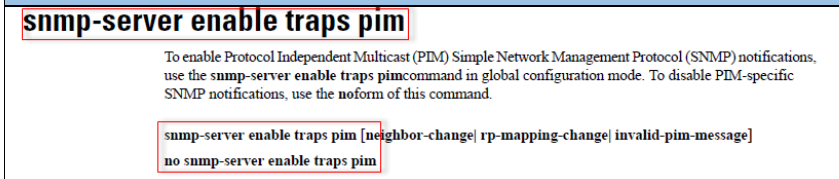
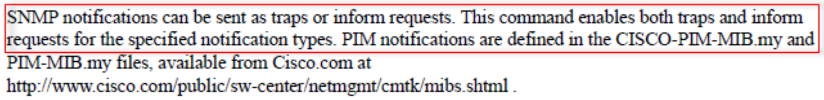
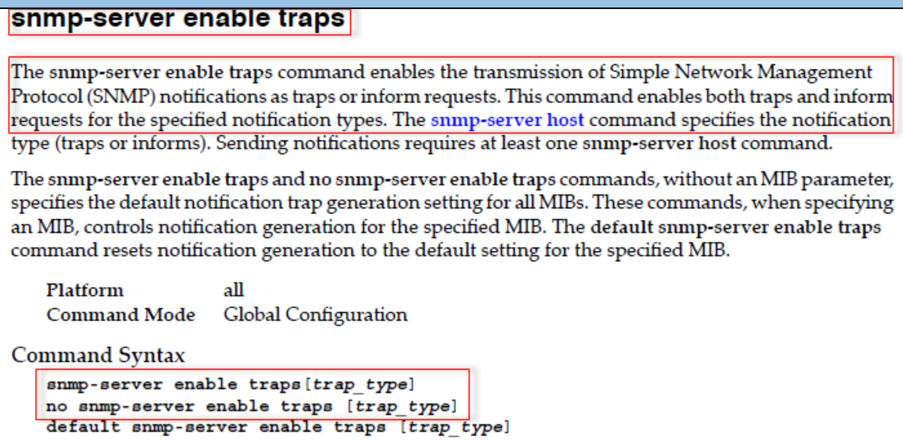
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Command** — **Description** **ip host** — Defines a static host name-to-address mapping in the host cache. **mls rp ip multicast** — Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch. **show ip mroute** — Displays the contents of the IP multicast routing table. Cisco IOS Multicast Command Reference (2013), at 21.	 **show ip mroute count** The show ip mroute count command displays IP multicast routing table statistics, including number of packets, packets per second, average packet size, and bits per second. The show ip mroute command displays the contents of the IP multicast routing table. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1773 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1500; Arista User Manual, v. 4.11.1 (1/11/13), at 1199; Arista User Manual v. 4.10.3 (10/22/12), at 1023; Arista User Manual v. 4.9.3.2 (5/3/12), at 781; Arista User Manual v. 4.8.2 (11/18/11), at 600; Arista User Manual v. 4.7.3 (7/18/11), at 479; Arista User Manual v. 4.6.0 (12/22/2010), at 326.	Dkt. 419-10 at PDF p. 126

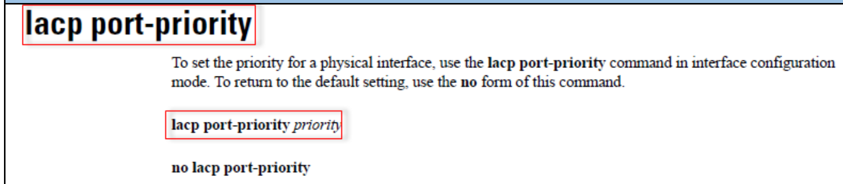
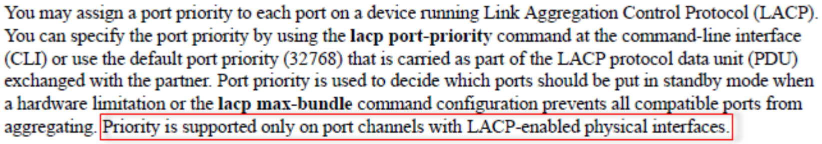
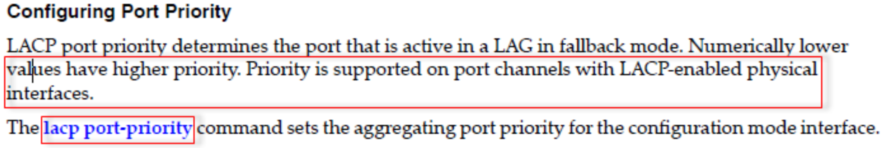

show ip igmp snooping
To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the **show ip igmp snooping**command in user EXEC or privileged EXEC mode.
show ip igmp snooping [**groups** [**count**| **vlan** *vlan-id* [*ip-address*| **count**]]| **mrouter** [[**vlan** *vlan-id*]| [**bd** *bd-id*]] | **querier**| **vlan** *vlan-id*| **bd** *bd-id*]
 	
Cisco IOS Multicast Command Reference at 625 (2013).
 	

The following is sample output from the **show ip igmp snooping** command:
`Router# show ip igmp snooping`
`Global IGMP Snooping configuration:`
`-----------------------------------`
`IGMP snooping              : Enabled`
`IGMPv3 snooping (minimal)  : Enabled`
`Report suppression         : Enabled`
`TCN solicit query          : Disabled`
`TCN flood query count      : 2`
`Last Member Query Interval : 1000`
 	
IOS Multicast Command Reference (2013), at 625.
	
	IGMP Snooping Status
	The show ip igmp snooping command displays the Internet Group Management Protocol (IGMP) snooping configuration of a device.
	Example
	- This command displays the switch's IGMP snooping configuration.
	`switch>show ip igmp snooping`
	`   Global IGMP Snooping configuration:`
	`-------------------------------------------`
	`IGMP snooping                  : Enabled`
	`Robustness variable            : 2`
	
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1785.
	
	See also Arista User Manual v. 4.12.3 (7/17/13), at 1511; Arista User Manual, v. 4.11.1 (1/11/13), at 1255; Arista User Manual v. 4.10.3 (10/22/12), at 1066; Arista User Manual v. 4.9.3.2 (5/3/12), at 824; Arista User Manual v. 4.8.2 (11/18/11), at 630; Arista User Manual v. 4.7.3 (7/18/11), at 505; Arista User Manual v. 4.6.0 (12/22/2010), at 351.
		Dkt. 419-10 at PDF p. 126

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **show ip igmp snooping mrouter** Note: The documentation for this command has been integrated into the documentation for the **show ip igmp snooping** command. Please see the **show ip igmp snooping** command for complete and up-to-date information about displaying information for dynamically learned and manually configured multicast router ports. To display information on dynamically learned and manually configured multicast router ports, use the **show ip igmp snooping mrouter**command in privileged EXEC mode. **show ip igmp snooping mrouter** {**vlan** *vlan-id*| **bd** *bd-id*} Syntax Description **vlan** *vlan-id* — Specifies a VLAN. Valid values are 1 to 1001. **bd** *bd-id* — Specifies a bridge domain. Valid values are 1 to 16823. Cisco IOS Multicast Command Reference (2013), at 634.	 **show ip igmp snooping mrouter** The show ip igmp snooping mrouter command displays information on dynamically learned and manually configured multicast router ports. Command provides options to include only specific VLANs. Platform all Command Mode EXEC Command Syntax `show ip igmp snooping mrouter [VLAN_ID] [DATA]` Parameters • *VLAN_ID* specifies VLAN for which command displays information. Options include: — <no parameter> all VLANs. — vlan *v_num* specified VLAN. • *DATA* specifies the type of information displayed. Options include: — <no parameter> displays VLAN number and port-list for each group. — detail displays port-specific data for each group; includes transmission times and expiration. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1859 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1567; Arista User Manual, v. 4.11.1 (1/11/13), at 1262; Arista User Manual v. 4.10.3 (10/22/12), at 1073; Arista User Manual v. 4.9.3.2 (5/3/12), at 830; Arista User Manual v. 4.8.2 (11/18/11), at 636; Arista User Manual v. 4.7.3 (7/18/11), at 511.	Dkt. 419-10 at PDF p. 127

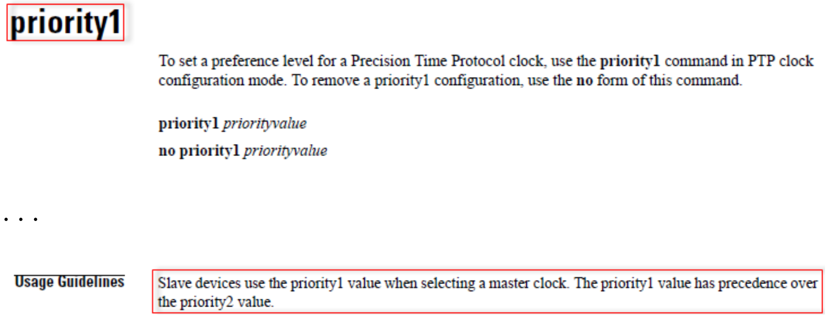
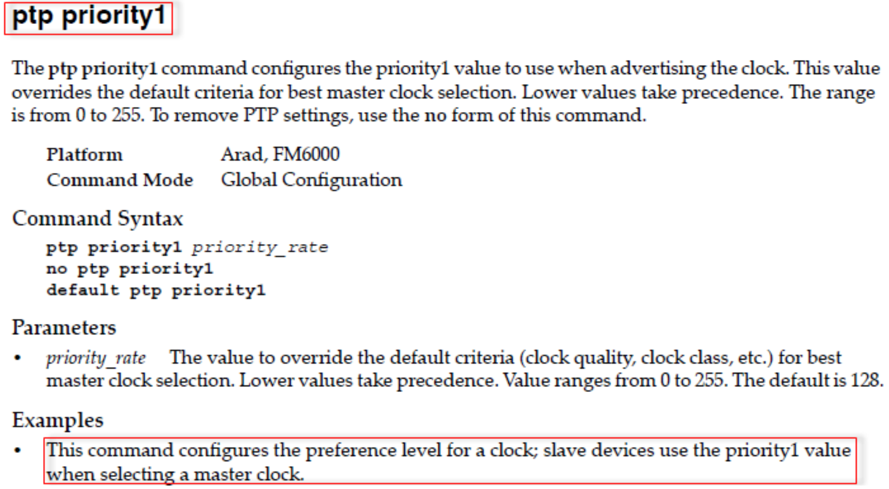
<table>
<tr><th>Cisco’s Documentation</th><th>Arista’s Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>
show ip mfib
To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib** command in user EXEC or privileged EXEC mode.
show ip mfib [**vrf** {*vrf-name*| *}] [**all**| **linkscope**| *group-address/mask*| *group-address* [*source-address*]| *source-address group-address*] [**verbose**]
Cisco IOS Multicast Command Reference (2013) at 649.</td>
<td>
show ip mfib
The show ip mfib command displays the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for hardware forwarded routes. Parameters options are available to filter output by group address or group and source addresses
Platform all
Command Mode EXEC
Command Syntax
`show ip mfib [ROUTE]`
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1770
See also Arista User Manual v. 4.12.3 (7/17/13), at 1497; Arista User Manual, v. 4.11.1 (1/11/13), at 1196; Arista User Manual v. 4.10.3 (10/22/12), at 1020; Arista User Manual v. 4.9.3.2 (5/3/12), at 778; Arista User Manual v. 4.8.2 (11/18/11), at 597; Arista User Manual v. 4.7.3 (7/18/11), at 477; Arista User Manual v. 4.6.0 (12/22/2010), at 324.</td>
<td>Dkt. 419-10 at PDF p. 128</td>
</tr>
</table>

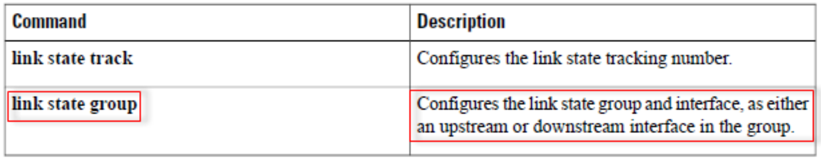
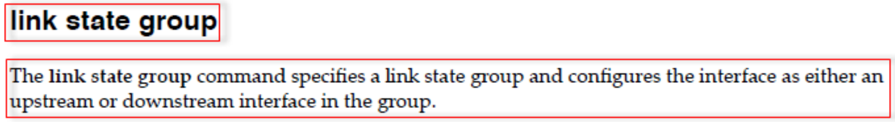
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


snmp-server enable traps pim
To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim**command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no**form of this command.
snmp-server enable traps pim [neighbor-change| rp-mapping-change| invalid-pim-message]
no snmp-server enable traps pim
Cisco IOS Multicast Command Reference (2013), at 950.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .
Cisco IOS Multicast Command Reference (2013), at 951.
	
	snmp-server enable traps
	The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command.
	The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
	Platform all
	Command Mode Global Configuration
	Command Syntax
	`snmp-server enable traps[trap_type]`
	`no snmp-server enable traps [trap_type]`
	`default snmp-server enable traps [trap_type]`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 1990.
	See also Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.
		Dkt. 419-10 at PDF p. 129

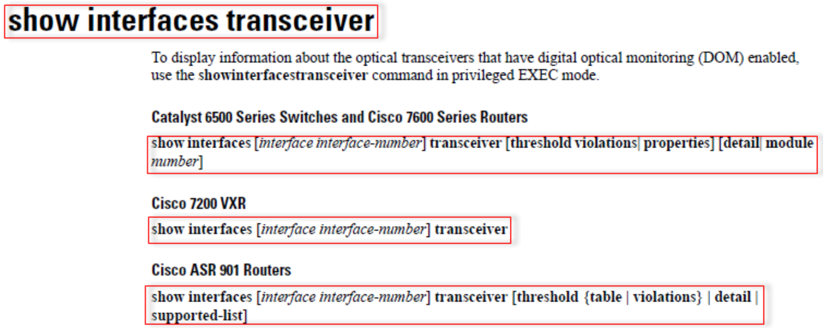
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **lacp port-priority** To set the priority for a physical interface, use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command. **lacp port-priority** *priority* **no lacp port-priority** Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 690.  You may assign a port priority to each port on a device running Link Aggregation Control Protocol (LACP). You can specify the port priority by using the **lacp port-priority** command at the command-line interface (CLI) or use the default port priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. Port priority is used to decide which ports should be put in standby mode when a hardware limitation or the **lacp max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces. Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 691.	 **Configuring Port Priority** LACP port priority determines the port that is active in a LAG in fallback mode. Numerically lower values have higher priority. Priority is supported on port channels with LACP-enabled physical interfaces. The lacp port-priority command sets the aggregating port priority for the configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 461. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 333; Arista User Manual v. 4.10.3 (10/22/12), at 291; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 207.	Dkt. 419-10 at PDF p. 130

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


priority1
To set a preference level for a Precision Time Protocol clock, use the **priority1** command in PTP clock configuration mode. To remove a priority1 configuration, use the **no** form of this command.
priority1 *priorityvalue*
no priority1 *priorityvalue*
. . .
Usage Guidelines Slave devices use the priority1 value when selecting a master clock. The priority1 value has precedence over the priority2 value.
Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1003.
	
	ptp priority1
	The ptp priority1 command configures the priority1 value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the no form of this command.
	Platform Arad, FM6000
	Command Mode Global Configuration
	Command Syntax
	`ptp priority1 priority_rate`
	`no ptp priority1`
	`default ptp priority1`
	Parameters
	• *priority_rate* The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128.
	Examples
	• This command configures the preference level for a clock; slave devices use the priority1 value when selecting a master clock.
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 326.
	See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.
		Dkt. 419-10 at PDF p. 131

 **Command** — **Description** **link state track** — Configures the link state tracking number. **link state group** — Configures the link state group and interface, as either an upstream or downstream interface in the group. Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1950.	 **link state group** The link state group command specifies a link state group and configures the interface as either an upstream or downstream interface in the group. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 659. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 527; Arista User Manual, v. 4.11.1 (1/11/13), at 422.	Dkt. 419-10 at PDF p. 131

Cisco's Documentation



show interfaces transceiver

To display information about the optical transceivers that have digital optical monitoring (DOM) enabled, use the showinterfacestransceiver command in privileged EXEC mode.

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

show interfaces [*interface interface-number*] **transceiver** [**threshold violations**| **properties**] [**detail**| **module** *number*]

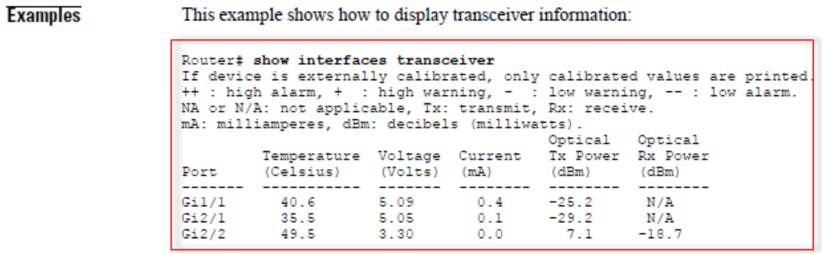
Cisco 7200 VXR

show interfaces [*interface interface-number*] **transceiver**

Cisco ASR 901 Routers

show interfaces [*interface interface-number*] **transceiver** [**threshold** {**table** | **violations**} | **detail** | **supported-list**]

Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1878.



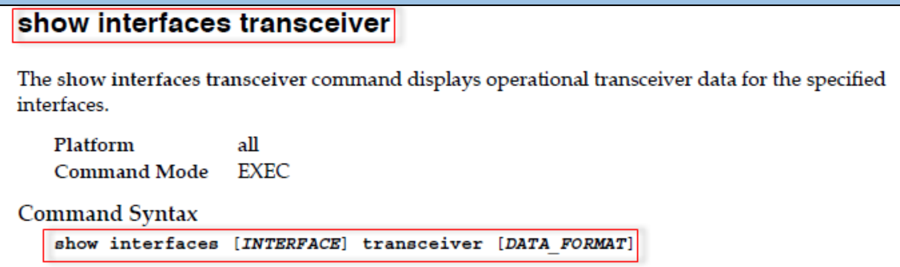
Examples

This example shows how to display transceiver information:

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                                Optical    Optical
         Temperature  Voltage  Current   Tx Power   Rx Power
Port     (Celsius)    (Volts)  (mA)      (dBm)      (dBm)
-------  -----------  -------  --------  --------   --------
Gi1/1      40.6       5.09       0.4     -25.2       N/A
Gi2/1      35.5       5.05       0.1     -29.2       N/A
Gi2/2      49.5       3.30       0.0       7.1      -18.7
```

Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1879.

Arista's Documentation



show interfaces transceiver

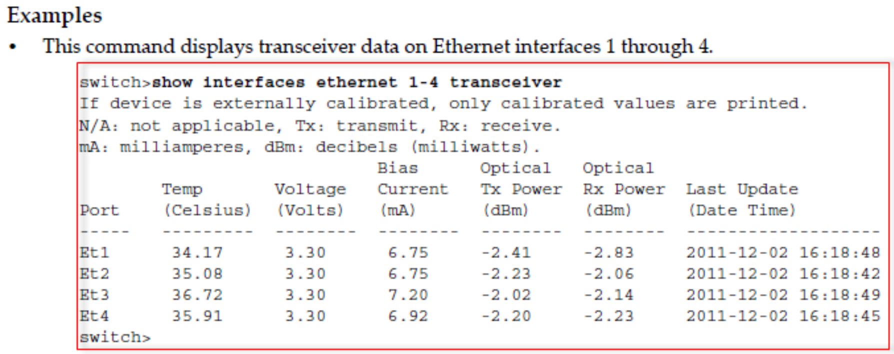
The show interfaces transceiver command displays operational transceiver data for the specified interfaces.

Platform	all
Command Mode	EXEC

Command Syntax

```
show interfaces [INTERFACE] transceiver [DATA_FORMAT]
```

. . .



Examples

- This command displays transceiver data on Ethernet interfaces 1 through 4.

```
switch>show interfaces ethernet 1-4 transceiver
If device is externally calibrated, only calibrated values are printed.
N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                             Bias      Optical   Optical
        Temp      Voltage    Current   Tx Power  Rx Power  Last Update
Port    (Celsius) (Volts)    (mA)      (dBm)     (dBm)     (Date Time)
-----   --------- --------   --------  --------  --------  -------------------
Et1      34.17     3.30       6.75     -2.41     -2.83     2011-12-02 16:18:48
Et2      35.08     3.30       6.75     -2.23     -2.06     2011-12-02 16:18:42
Et3      36.72     3.30       7.20     -2.02     -2.14     2011-12-02 16:18:49
Et4      35.91     3.30       6.92     -2.20     -2.23     2011-12-02 16:18:45
switch>
```

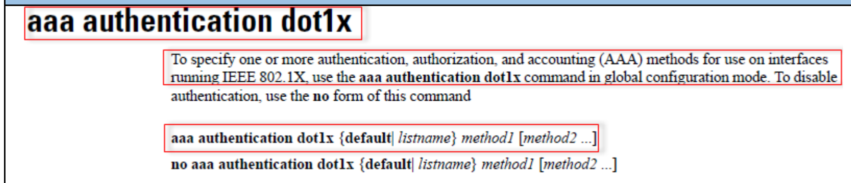
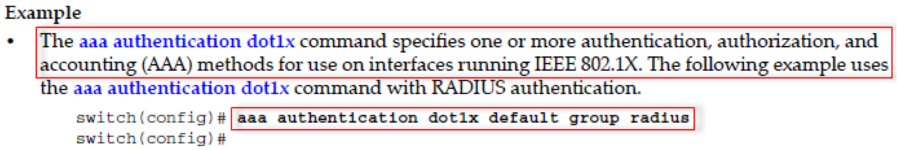
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 451.

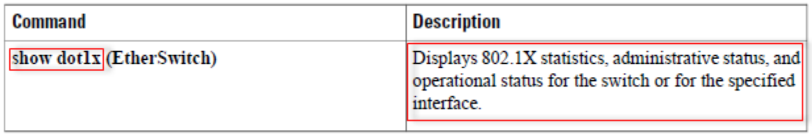
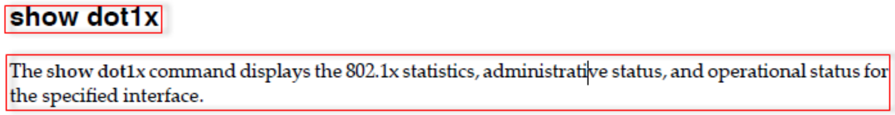
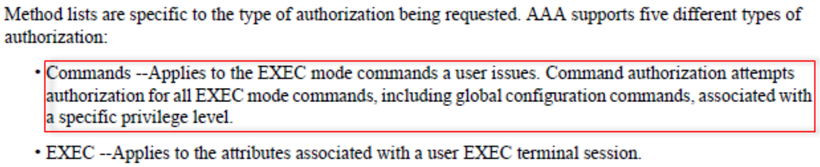
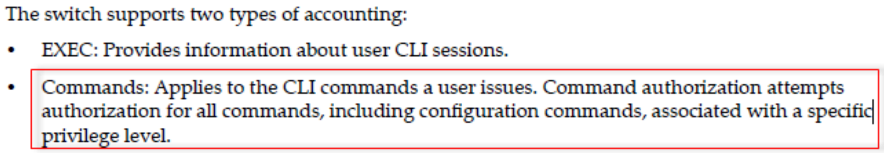
See also Arista User Manual v. 4.12.3 (7/17/13), at 385; Arista User Manual, v. 4.11.1 (1/11/13), at 326; Arista User Manual v. 4.10.3 (10/22/12), at 284; Arista User Manual v. 4.9.3.2 (5/3/12), at 266.

Supporting Evidence In The Record

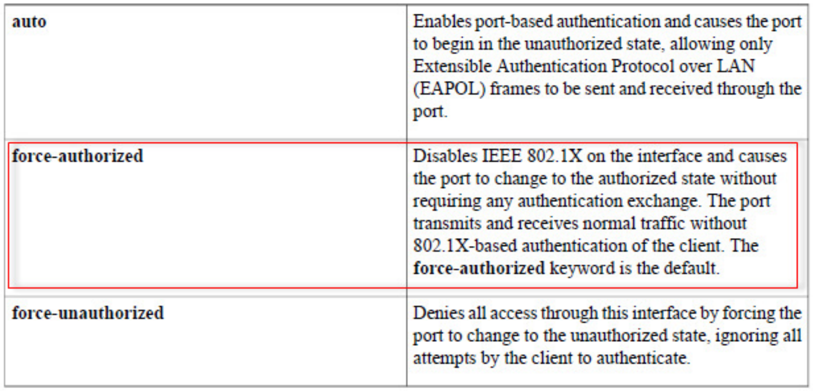
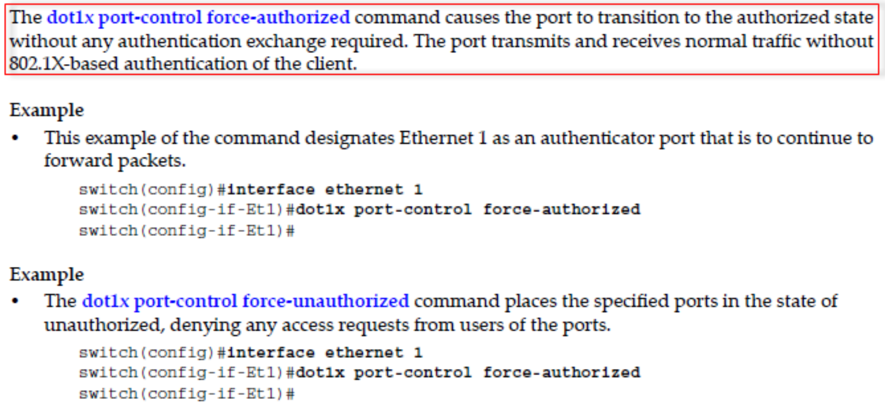
Dkt. 419-10 at PDF p. 132

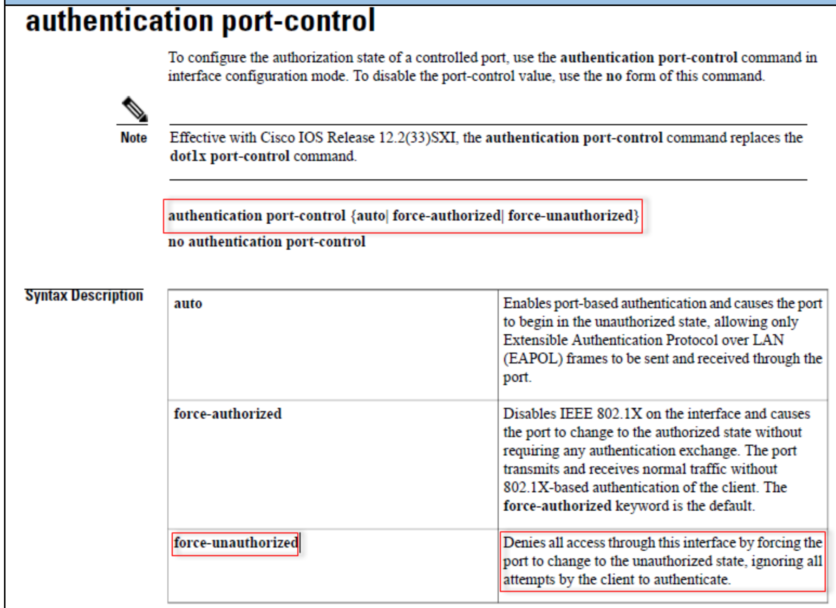
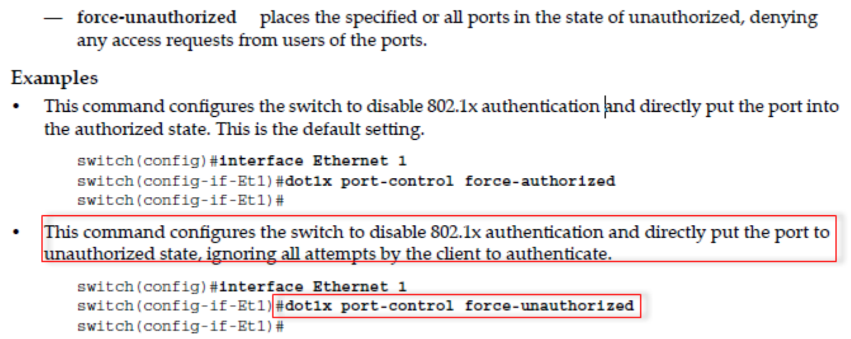
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record

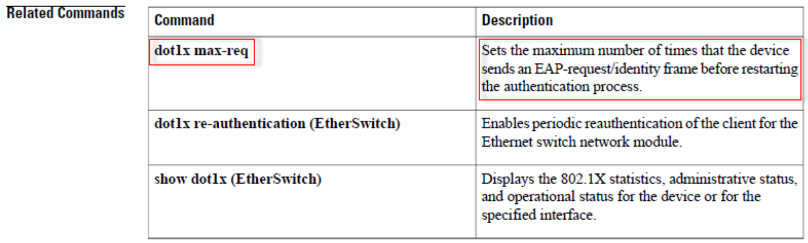
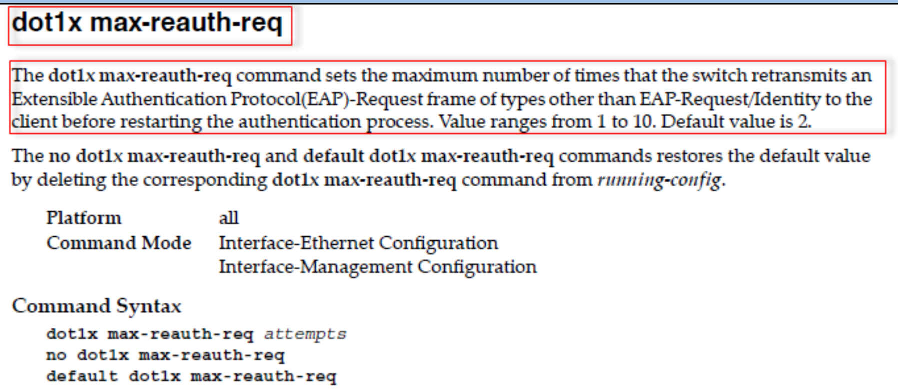
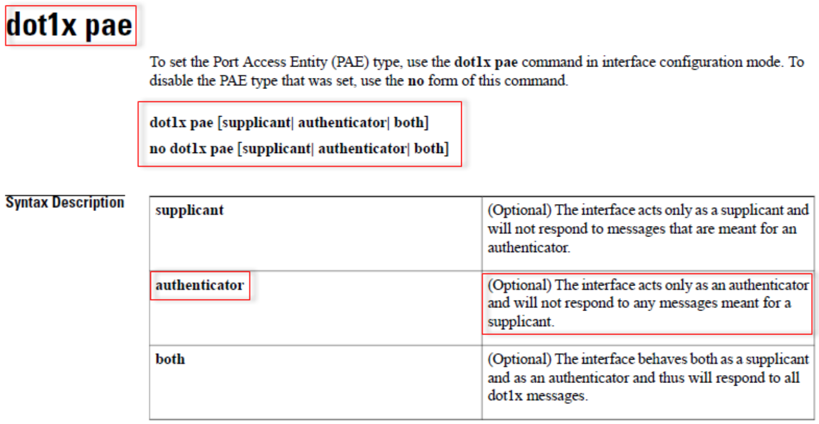
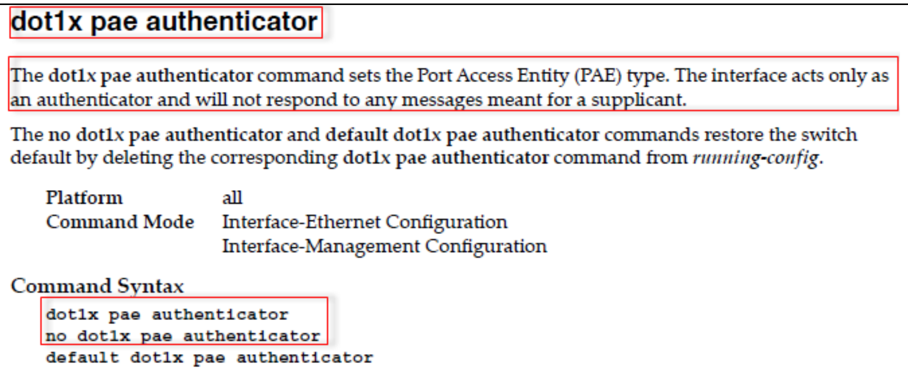

aaa authentication dot1x
To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command
aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]
no aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]
Cisco IOS Security Command Reference: Commands A to C (2013), at 54.
	
	Example
	• The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication.
	`switch(config)# aaa authentication dot1x default group radius`
	`switch(config)#`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 557.
		Dkt. 419-10 at PDF p. 133

 **Command** — **Description** **show dot1x** (EtherSwitch) — Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface. Cisco IOS Security Command Reference: Commands A to C (2013), at 56.	 **show dot1x** The show dot1x command displays the 802.1x statistics, administrative status, and operational status for the specified interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 572.	Dkt. 419-10 at PDF p. 133
 Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization: • Commands --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. • EXEC --Applies to the attributes associated with a user EXEC terminal session. Cisco IOS Security Command Reference: Commands A to C (2013), at 83.	 The switch supports two types of accounting: • EXEC: Provides information about user CLI sessions. • Commands: Applies to the CLI commands a user issues. Command authorization attempts authorization for all commands, including configuration commands, associated with a specific privilege level. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 207. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 154; Arista User Manual, v. 4.11.1 (1/11/13), at 114; Arista User Manual v. 4.10.3 (10/22/12), at 106; Arista User Manual v. 4.9.3.2 (5/3/12), at 93; Arista User Manual v. 4.8.2 (11/18/11), at 87; Arista User Manual v. 4.7.3 (7/18/11), at 73.	Dkt. 419-10 at PDF p. 133

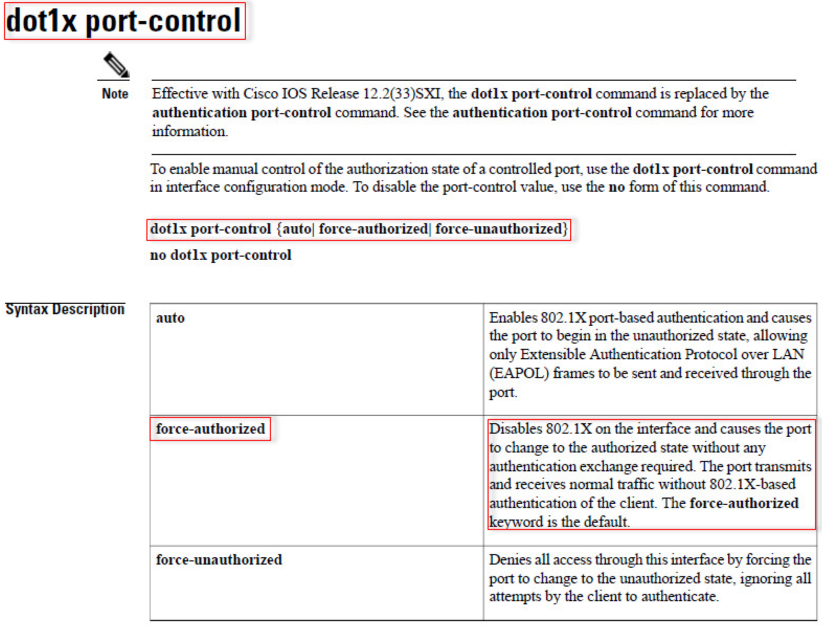
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


auto — Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized — Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized — Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.
 	
Cisco IOS Security Command Reference: Commands A to C (2013), at 354.
	
	The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
	
	Example
	- This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets.
	`switch(config)#interface ethernet 1`
	`switch(config-if-Et1)#dot1x port-control force-authorized`
	`switch(config-if-Et1)#`
	
	Example
	- The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports.
	`switch(config)#interface ethernet 1`
	`switch(config-if-Et1)#dot1x port-control force-authorized`
	`switch(config-if-Et1)#`
	
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 558.
		Dkt. 419-10 at PDF p. 134

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>
authentication port-control
To configure the authorization state of a controlled port, use the <b>authentication port-control</b> command in interface configuration mode. To disable the port-control value, use the <b>no</b> form of this command.
Note Effective with Cisco IOS Release 12.2(33)SXI, the <b>authentication port-control</b> command replaces the <b>dot1x port-control</b> command.
<b>authentication port-control</b> {<b>auto</b>| <b>force-authorized</b>| <b>force-unauthorized</b>}
<b>no authentication port-control</b>
Syntax Description<table><tr><td><b>auto</b></td><td>Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.</td></tr><tr><td><b>force-authorized</b></td><td>Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The <b>force-authorized</b> keyword is the default.</td></tr><tr><td><b>force-unauthorized</b></td><td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.</td></tr></table>
Cisco IOS Security Command Reference: Commands A to C (2013), at 354.</td>
<td>
— <b>force-unauthorized</b> places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.
Examples
• This command configures the switch to disable 802.1x authentication and directly put the port into the authorized state. This is the default setting.
switch(config)#<b>interface Ethernet 1</b>
switch(config-if-Et1)#<b>dot1x port-control force-authorized</b>
switch(config-if-Et1)#
• This command configures the switch to disable 802.1x authentication and directly put the port to unauthorized state, ignoring all attempts by the client to authenticate.
switch(config)#<b>interface Ethernet 1</b>
switch(config-if-Et1)#<b>dot1x port-control force-unauthorized</b>
switch(config-if-Et1)#
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 567.</td>
<td>Dkt. 419-10 at PDF p. 135</td>
</tr>
</table>

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

Related Commands
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>dot1x max-req</td><td>Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.</td></tr>
<tr><td>dot1x re-authentication (EtherSwitch)</td><td>Enables periodic reauthentication of the client for the Ethernet switch network module.</td></tr>
<tr><td>show dot1x (EtherSwitch)</td><td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td></tr>
</table>
Cisco IOS Security Command Reference: Commands D to L (2013), at 219.
</td>
<td>

dot1x max-reauth-req
The dot1x max-reauth-req command sets the maximum number of times that the switch retransmits an Extensible Authentication Protocol(EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process. Value ranges from 1 to 10. Default value is 2.
The no dot1x max-reauth-req and default dot1x max-reauth-req commands restores the default value by deleting the corresponding dot1x max-reauth-req command from running-config.
Platform all
Command Mode Interface-Ethernet Configuration
Interface-Management Configuration
Command Syntax
dot1x max-reauth-req attempts
no dot1x max-reauth-req
default dot1x max-reauth-req
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 565.
</td>
<td>Dkt. 419-10 at PDF p. 136</td>
</tr>
<tr>
<td>

dot1x pae
To set the Port Access Entity (PAE) type, use the dot1x pae command in interface configuration mode. To disable the PAE type that was set, use the no form of this command.
dot1x pae [supplicant| authenticator| both]
no dot1x pae [supplicant| authenticator| both]
Syntax Description
<table>
<tr><td>supplicant</td><td>(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.</td></tr>
<tr><td>authenticator</td><td>(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</td></tr>
<tr><td>both</td><td>(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.</td></tr>
</table>
Cisco IOS Security Command Reference: Commands D to L (2013), at 195.
</td>
<td>

dot1x pae authenticator
The dot1x pae authenticator command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
The no dot1x pae authenticator and default dot1x pae authenticator commands restore the switch default by deleting the corresponding dot1x pae authenticator command from running-config.
Platform all
Command Mode Interface-Ethernet Configuration
Interface-Management Configuration
Command Syntax
dot1x pae authenticator
no dot1x pae authenticator
default dot1x pae authenticator
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 567.
</td>
<td>Dkt. 419-10 at PDF p. 136</td>
</tr>
</table>

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr><td>



dot1x port-control

Note: Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x port-control** command is replaced by the **authentication port-control** command. See the **authentication port-control** command for more information.

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

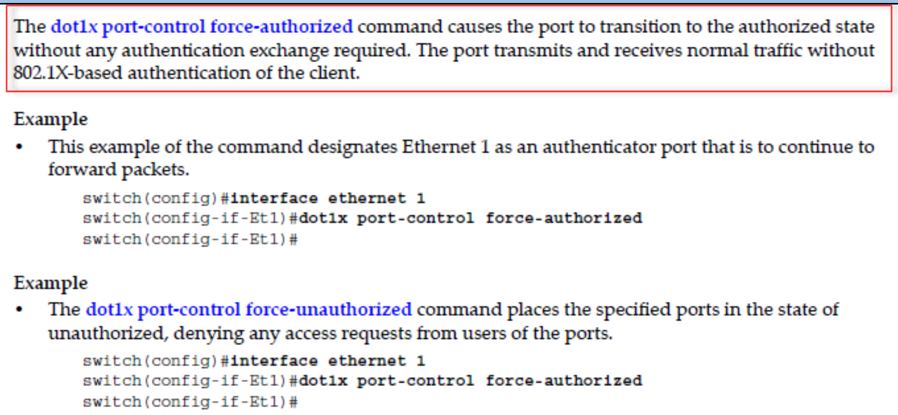
no dot1x port-control

Syntax Description

auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Cisco IOS Security Command Reference: Commands D to L (2013), at 197.

</td><td>



The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.

Example

- This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets.

```
switch(config)#interface ethernet 1
switch(config-if-Et1)#dot1x port-control force-authorized
switch(config-if-Et1)#
```

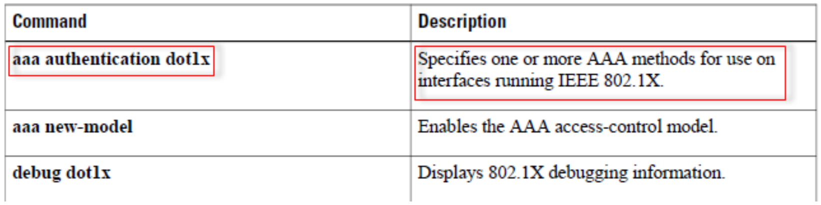
Example

- The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports.

```
switch(config)#interface ethernet 1
switch(config-if-Et1)#dot1x port-control force-authorized
switch(config-if-Et1)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 558.

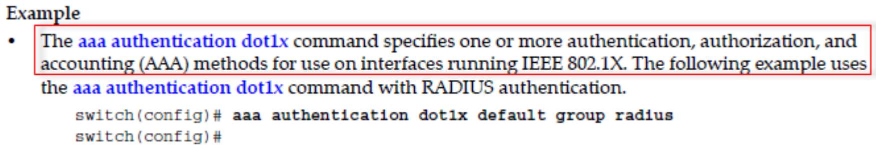
</td><td>Dkt. 419-10 at PDF p. 137</td></tr>
<tr><td>



Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.

Cisco IOS Security Command Reference: Commands D to L (2013), at 211.

</td><td>



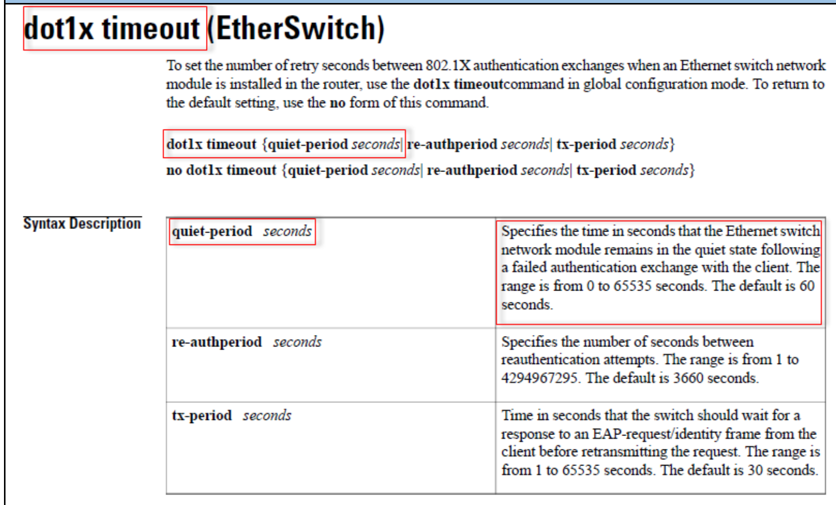
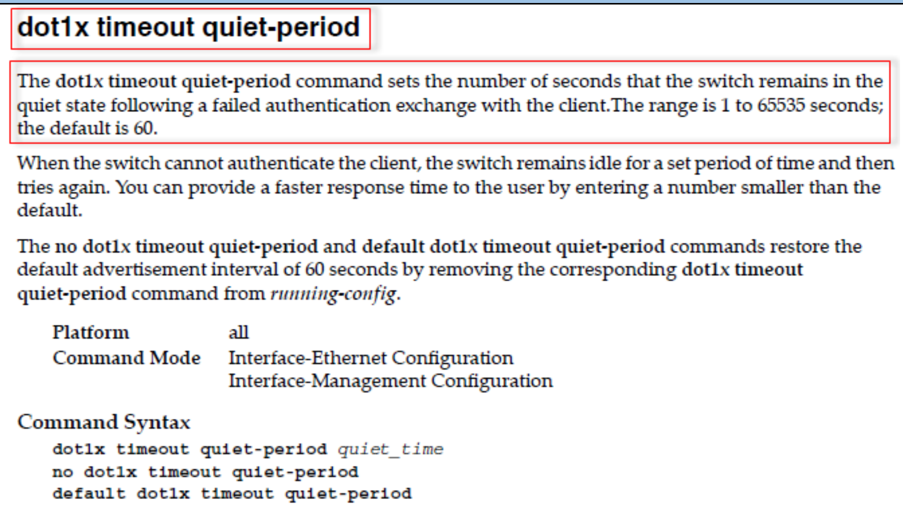
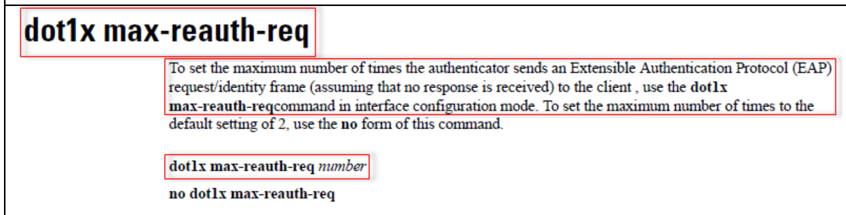
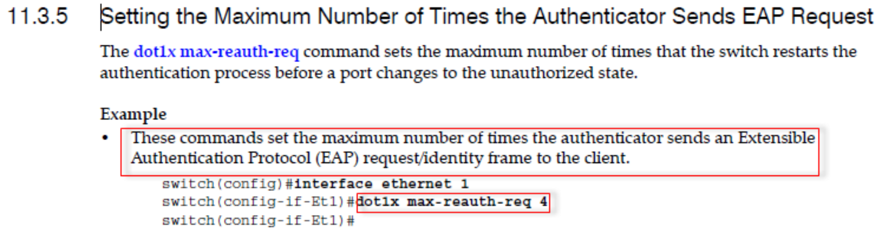
Example

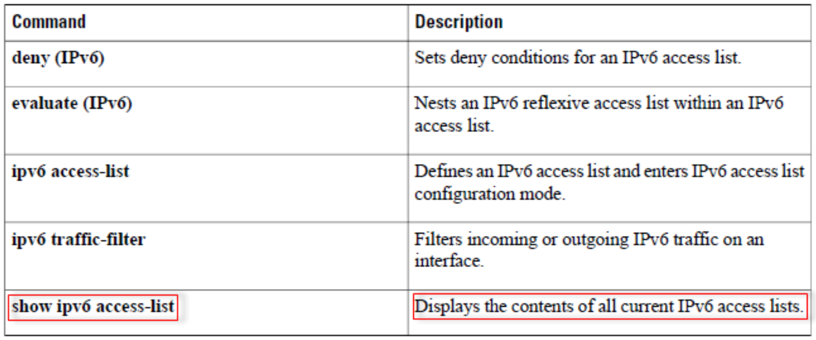
- The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication.

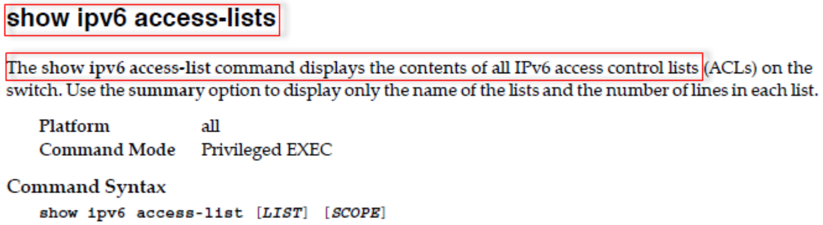
```
switch(config)# aaa authentication dot1x default group radius
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 557.

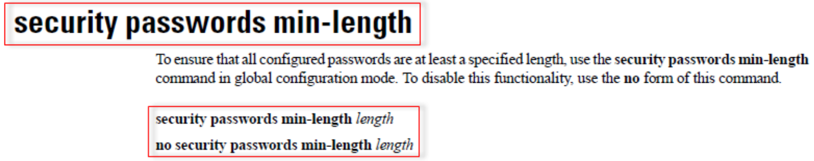
</td><td>Dkt. 419-10 at PDF p. 137</td></tr>
</table>

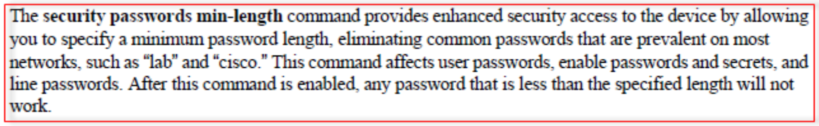
<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>
dot1x timeout (EtherSwitch)
To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the <b>dot1x timeout</b>command in global configuration mode. To return to the default setting, use the <b>no</b> form of this command.
<b>dot1x timeout</b> {<b>quiet-period</b> <i>seconds</i>| <b>re-authperiod</b> <i>seconds</i>| <b>tx-period</b> <i>seconds</i>}
<b>no dot1x timeout</b> {<b>quiet-period</b> <i>seconds</i>| <b>re-authperiod</b> <i>seconds</i>| <b>tx-period</b> <i>seconds</i>}
Syntax Description
<table>
<tr><td><b>quiet-period</b> <i>seconds</i></td><td>Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.</td></tr>
<tr><td><b>re-authperiod</b> <i>seconds</i></td><td>Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.</td></tr>
<tr><td><b>tx-period</b> <i>seconds</i></td><td>Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.</td></tr>
</table>
Cisco IOS Security Command Reference: Commands D to L (2013), at 218.</td>
<td>
dot1x timeout quiet-period
The <b>dot1x timeout quiet-period</b> command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60.
When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.
The <b>no dot1x timeout quiet-period</b> and <b>default dot1x timeout quiet-period</b> commands restore the default advertisement interval of 60 seconds by removing the corresponding <b>dot1x timeout quiet-period</b> command from <i>running-config</i>.
Platform all
Command Mode Interface-Ethernet Configuration
Interface-Management Configuration
Command Syntax
<b>dot1x timeout quiet-period</b> <i>quiet_time</i>
<b>no dot1x timeout quiet-period</b>
<b>default dot1x timeout quiet-period</b>
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 569.</td>
<td>Dkt. 419-10 at PDF p. 138</td>
</tr>
<tr>
<td>
dot1x max-reauth-req
To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client , use the <b>dot1x max-reauth-req</b>command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the <b>no</b> form of this command.
<b>dot1x max-reauth-req</b> <i>number</i>
<b>no dot1x max-reauth-req</b>
Cisco IOS Security Command Reference: Commands D to L (2013), at 185.</td>
<td>
11.3.5 Setting the Maximum Number of Times the Authenticator Sends EAP Request
The <b>dot1x max-reauth-req</b> command sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
Example
• These commands set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame to the client.
switch(config)#<b>interface ethernet 1</b>
switch(config-if-Et1)#<b>dot1x max-reauth-req 4</b>
switch(config-if-Et1)#
Arista User Manual v. 4.14.3F – Rev. 2 (10/2/14), at 559.</td>
<td>Dkt. 419-10 at PDF p. 138</td>
</tr>
</table>

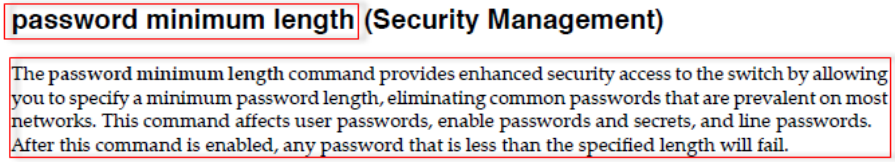
<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>deny (IPv6)</td><td>Sets deny conditions for an IPv6 access list.</td></tr>
<tr><td>evaluate (IPv6)</td><td>Nests an IPv6 reflexive access list within an IPv6 access list.</td></tr>
<tr><td>ipv6 access-list</td><td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td></tr>
<tr><td>ipv6 traffic-filter</td><td>Filters incoming or outgoing IPv6 traffic on an interface.</td></tr>
<tr><td>show ipv6 access-list</td><td>Displays the contents of all current IPv6 access lists.</td></tr>
</table>

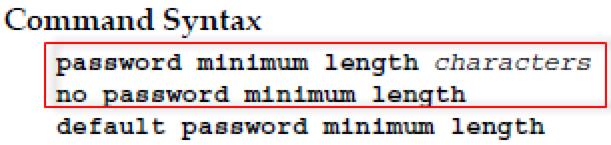
Cisco IOS Security Command Reference: Commands M to R at 440 (2013).
</td>
<td>

show ipv6 access-lists
The show ipv6 access-list command displays the contents of all IPv6 access control lists (ACLs) on the switch. Use the summary option to display only the name of the lists and the number of lines in each list.
Platform all
Command Mode Privileged EXEC
Command Syntax
show ipv6 access-list [LIST] [SCOPE]

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 904.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 782; Arista User Manual, v. 4.11.1 (1/11/13), at 611; Arista User Manual v. 4.10.3 (10/22/12), at 525.
</td>
<td>Dkt. 419-10 at PDF p. 139</td>
</tr>
<tr>
<td>

security passwords min-length
To ensure that all configured passwords are at least a specified length, use the <b>security passwords min-length</b> command in global configuration mode. To disable this functionality, use the <b>no</b> form of this command.
<b>security passwords min-length</b> <i>length</i>
<b>no security passwords min-length</b> <i>length</i>

. . .

The <b>security passwords min-length</b> command provides enhanced security access to the device by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco." This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will not work.

Cisco IOS Security Command Reference: Commands S to Z at 37 (2013).
</td>
<td>

password minimum length (Security Management)
The password minimum length command provides enhanced security access to the switch by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks. This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

. . .

Command Syntax
password minimum length <i>characters</i>
no password minimum length
default password minimum length

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 158.
</td>
<td>Dkt. 419-10 at PDF p. 139</td>
</tr>
</table>